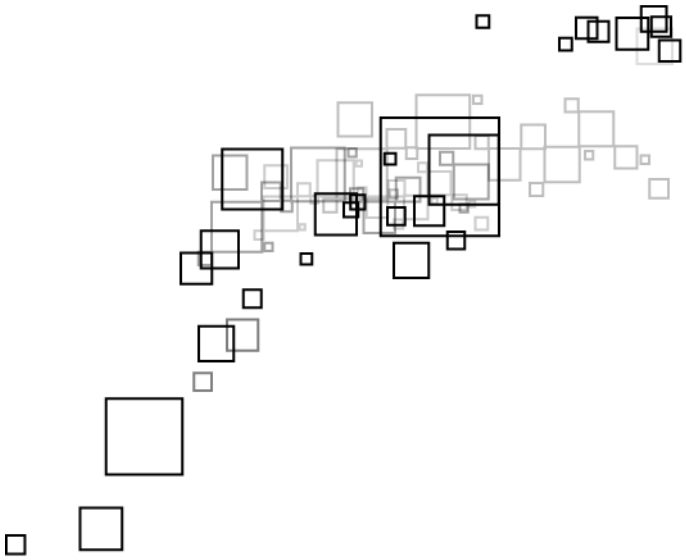


User Manual

WIPC302

Wireless N IP Camera

© Copyright 2011 All rights reserved. Ver 1.1

No part of this document may be reproduced, republished, or retransmitted in any form or by any means whatsoever, whether electronically or mechanically, including, but not limited to, by way of photocopying, recording, information recording, or through retrieval systems without the express written permission. We reserve the right to revise this document at any time without the obligation to notify any person and/or entity. All other company or product names mentioned are used for identification purposes only and may be trademarks of their respective owners.

LIMITATION OF LIABILITY AND DAMAGES

THE PRODUCT AND THE SOFTWARES WITHIN ARE PROVIDED "AS IS," BASIS. THE MANUFACTURER AND MANUFACTURER'S RESELLERS (COLLECTIVELY REFERRED TO AS "THE SELLERS") DISCLAIM ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, OR ANY WARRANTIES ARISING FROM COURSE OF DEALING, COURSE OF PERFORMANCE, OR USAGE OF TRADE. IN NO EVENT WILL THE SELLERS BE LIABLE FOR DAMAGES OR LOSS, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL WILLFUL, PUNITIVE, INCIDENTAL, EXEMPLARY, OR CONSEQUENTIAL, DAMAGES, DAMAGES FOR LOSS OF BUSINESS PROFITS, OR DAMAGES FOR LOSS OF BUSINESS OF ANY CUSTOMER OR ANY THIRD PARTY ARISING OUT OF THE USE OR THE INABILITY TO USE THE PRODUCT OR THE SOFTWARES, INCLUDING BUT NOT LIMITED TO THOSE RESULTING FROM DEFECTS IN THE PRODUCT OR SOFTWARE OR DOCUMENTATION, OR LOSS OR INACCURACY OF DATA OF ANY KIND, WHETHER BASED ON CONTRACT, TORT OR ANY OTHER LEGAL THEORY, EVEN IF THE PARTIES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE PRODUCT OR ITS SOFTWARE IS ASSUMED BY CUSTOMER. BECAUSE SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABLITY FOR DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO THE PARTIES. IN NO EVENT WILL THE SELLERS' TOTAL CUMULATIVE LIABILITY OF EACH AND EVERY KIND IN RELATION TO THE PRODUCT OR ITS SOFTWARE EXCEED THE AMOUNT PAID BY CUSTOMER FOR THE PRODUCT.

Table of Contents

About the Device....4
Requirements....5
Package Contents....5
Device Design....6
Getting Started....8
Planning Your Network....9
Remove or Disable Conflicts....10
Internet Sharing, Proxy, and Security Applications....10
Configuring TCP/IP Settings....11
Configuring Internet Properties....11
Removing Temporary Internet Files....12
Setup the Device....13
Installing the Utility....14
Requirements....14
Installation....14
About the Web User Interface....17
Menus....17
Home....18
Quick Setup....19
View....21
Network....23
Alarm....28
Advanced....32
Management....34
Multiple Device Monitoring System....38
Installation....38
Multiple Device Monitoring System WEB UI....41
Frequently Asked Questions....47

About the Device

Aztech WIPC302 is a Wireless N lite IP Camera that supports 802.11 b/g/n targeted at providing good video quality to the end users via wired and wireless connection. Wireless supports WEP/WPA /WPA2 encryption.

The video is compressed by MJPEG and allows user to change video resolution according to their demands to satisfy their own visual preferences.

With built-in Microphone, it enables user to monitor the sounds by connecting an external speaker to the IP camera. The device also supports two-way intercom function to allow user to communicate to the person on the other location.

With Motion detection, Alarm notification and Infrared feature, it allows user a 24 hours monitoring. The device can capture video snapshots to automatically send to your FTP server or send email notification.

Hassle free Manufacturer's DDNS which is unique for every device. The Web User Interface is accessible to any Web browser and mobile phone to view video anywhere. It supports three levels of user authority to access the Web User Interface.

WIPC302 supports dynamic UPnP* that allows port forwarding automatically on the router.

* Ensure that your router supports dynamic UPnP for this feature to work properly.

Requirements

Your computer must meet the following minimum requirements.

- Any operating system can be used
- Web Browser
- CD-ROM drive
- 233MHz processor
- Ethernet network adapter

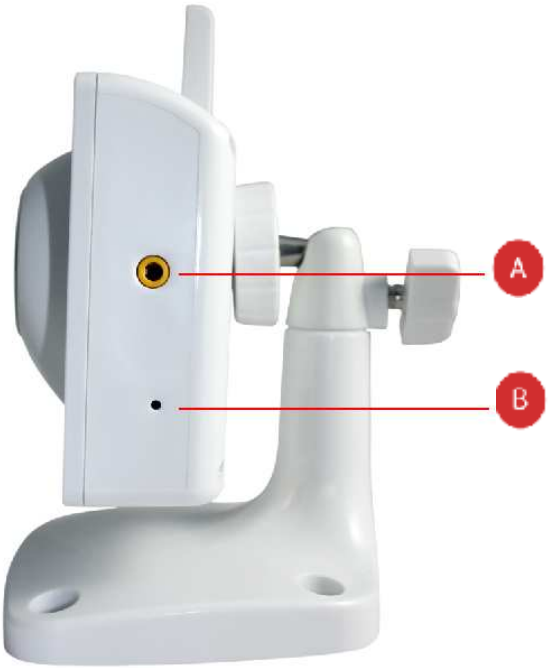
Package Contents

Package contents are listed below. For any missing items, please contact your dealer immediately. Product contents vary for different models.

- WIPC302
- Ethernet cable
- Camera Stand
- 5V 2.0A DC Power Adapter
- Easy Start Guide
- Resource CD
- Warranty Card

Device Design

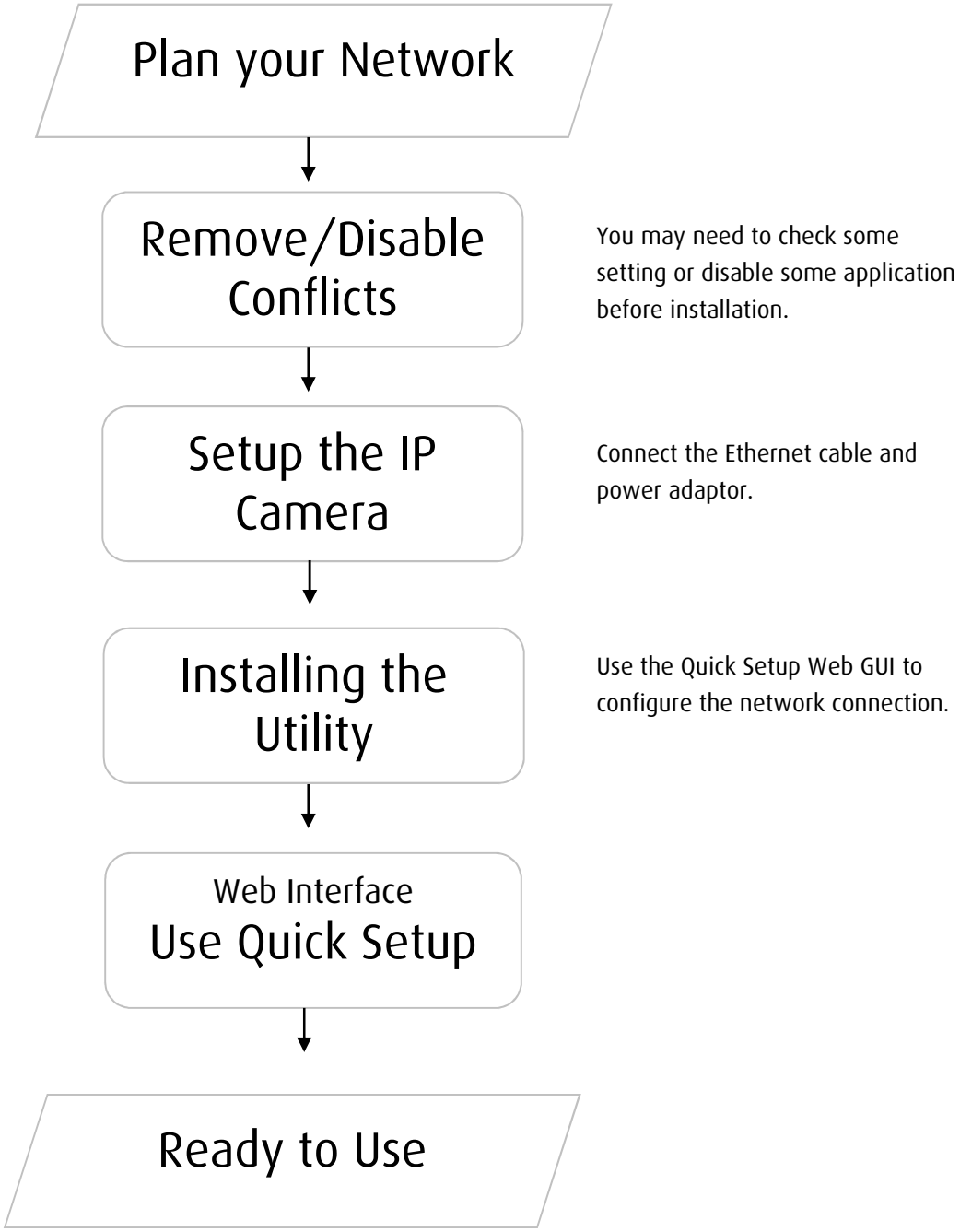
	Label	Description
A	Ethernet Port	Connect to your Modem/Router using an Ethernet cable.
B	Power Jack	Connect the 5v 1.5A Power adapter.
C	Camera Lens	CMOS sensor with fixed focus LENS.
D	Infrared LED	Automatically activates for night vision.
E	Light Sensor	Automatically activates Infrared LED for night vision.
F	Microphone	Built-in microphone.
G	Network LED	This LED blinks when there is activity
H	IP Camera Stand	
I	Antenna	Fixed Wireless Lite N antenna



	Label	Description
A	Audio out	Connect to your external speaker.
B	Reset	Press for 10 seconds or wait until the Network LED to stop blinking.

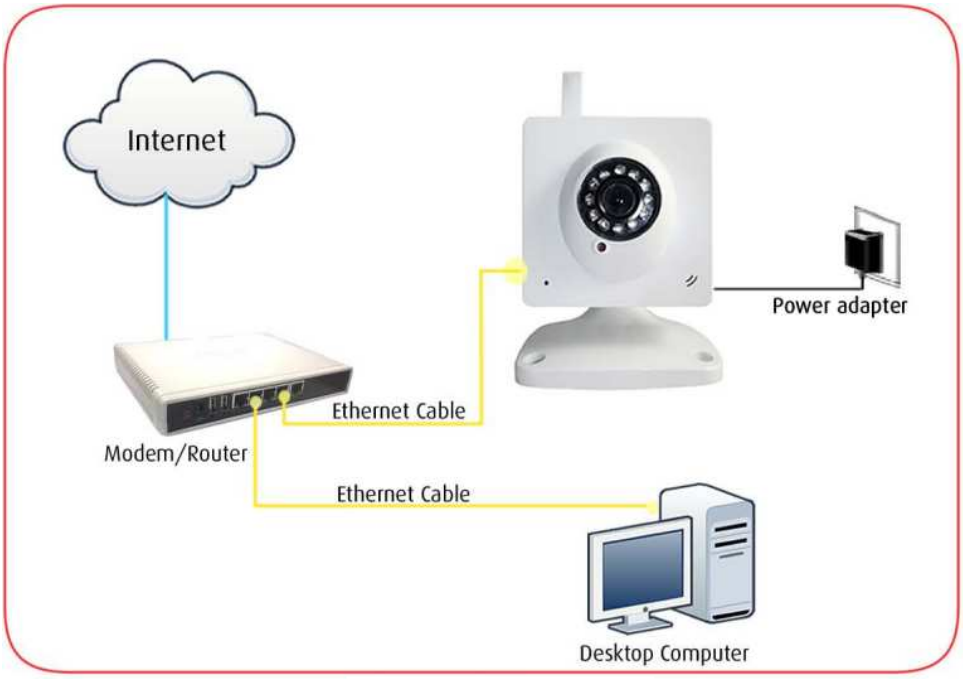
Getting Started

Setting up the device is easy. The flowchart below provides an outline of the steps needed to complete the installation. Brief descriptions appear beside each step. Detailed instructions are provided in the subsequent pages.


Plan your Network
Remove/Disable Conflicts
You may need to check some setting or disable some application before installation.
Setup the IP Camera
Connect the Ethernet cable and power adaptor.
Installing the Utility
Use the Quick Setup Web GUI to configure the network connection.
Web Interface
Use Quick Setup
Ready to Use

Planning Your Network

Before moving ahead to setup your network, it is a good idea to draw out a network diagram to help identify your network devices and plan out how to connect these devices. The illustration below is an example of a network diagram.



Wired Connection

Wireless Connection

Remove or Disable Conflicts

To make sure the router installation moves on smoothly, you need to remove or disable conflicts that may interfere the installation. Probable conflicts may include:

- Internet sharing applications
- Proxy software
- Security software
- TCP/IP settings
- Internet properties
- Temporary Internet files

Internet Sharing, Proxy, and Security Applications

Internet sharing, proxy software, and firewall applications may interfere with the router installation. These should be removed or disabled before start the installation.

If you have any of the following or similar applications installed on your computer, remove or disable them according to the manufacturer's instructions.

Internet Sharing Applications	Proxy Software	Security Software
Microsoft Internet Sharing	WinGate	Symantec
	WinProxy	Zone Alarm

Configuring TCP/IP Settings

Check if your computer uses the default TCP/IP settings.

To check the TCP/IP properties:

1. Select Start > Run. This opens the Run dialog box.
2. Enter control ncpa.cpl and then click OK. This opens the Network Connections in your computer.
3. Right-click LAN and then select Properties. This opens the Local Area Connection Properties dialog box.
4. Select Internet Protocol (TCP/IP) and then click Properties. This opens the Internet Protocol (TCP/IP) dialog box.
5. Select Obtain an IP address automatically.
6. Click OK to close the Internet Protocol (TCP/IP) dialog box.
7. Click OK to close the Local Area Connection Properties dialog box.

Configuring Internet Properties

To set the Internet Properties:

1. Select Start > Run. This opens the Run dialog box.
2. Enter control inetcpl.cpl and then click OK. This opens Internet Properties.
3. Click Connections tab.
4. In the Dial-up and Virtual Private Network settings pane, select Never dial a connection.
5. Click OK to close Internet Properties.

Removing Temporary Internet Files

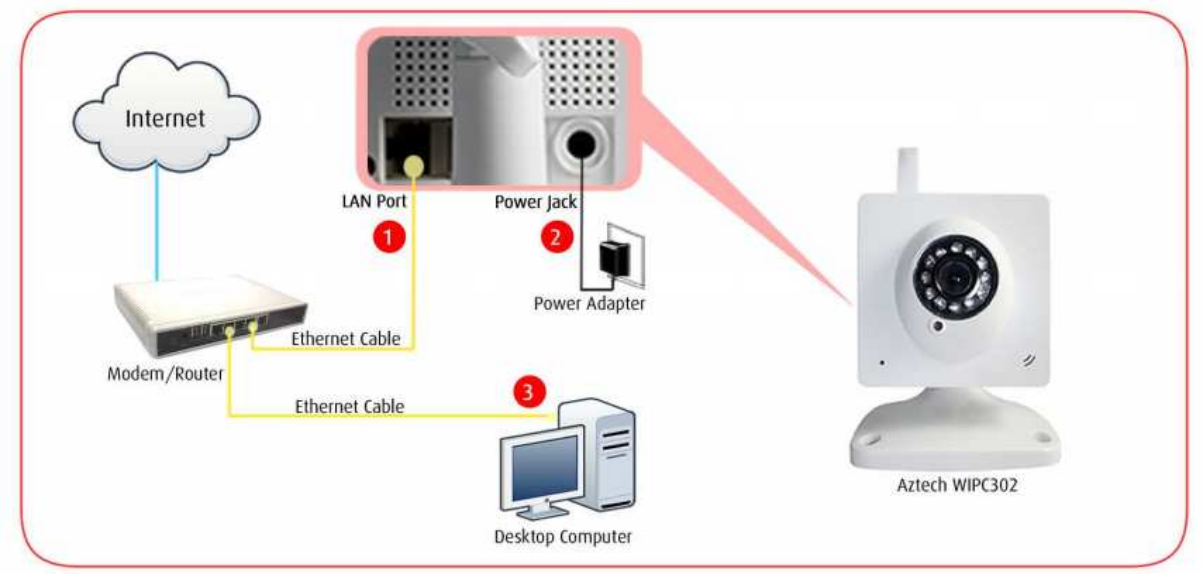
Temporary Internet files are files from Web sites that are stored in your computer. Delete these files to clean the cache and remove footprints left by the Web pages you visited.

To remove temporary Internet files:

1. Select Start > Run. This opens the Run dialog box.
2. Enter control and then click OK. This opens Control Panel.
3. Double-click Internet Options. This opens Internet Options.
4. In the Temporary Internet Files pane, click Delete Cookies.
5. Click Delete Files.
6. Click OK to close Internet Properties.

Setup the Device

When installing the IP Camera, find an area where there are enough electrical outlets for the IP Camera, router, the main computer, and your other Ethernet devices.



1. Connect your Aztech WIPC302 into your Modem/Router's Ethernet LAN port with an Ethernet cable.
2. Make user that your Modem/Router's Internet connection is UP to allow you to access your IP camera via the Internet.
3. Connect the Power Adapter to your Aztech WIPC302 and plug it into the power outlet then switch it ON.
4. Connect your computer to the same router wherein Aztech WIPC302 is connected then launch the WIPC302 utility.

Installing the Utility

WIPC302 Utility is a software application that allows you to configure your IP Camera.

Requirements

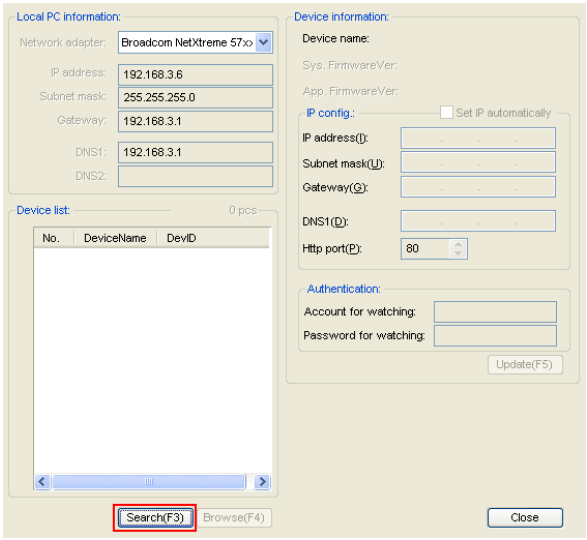
Your computer must meet the following minimum requirements.

- Any operating system can be used
- Web Browser
- CD-ROM drive
- 233MHz processor
- Ethernet network adapter

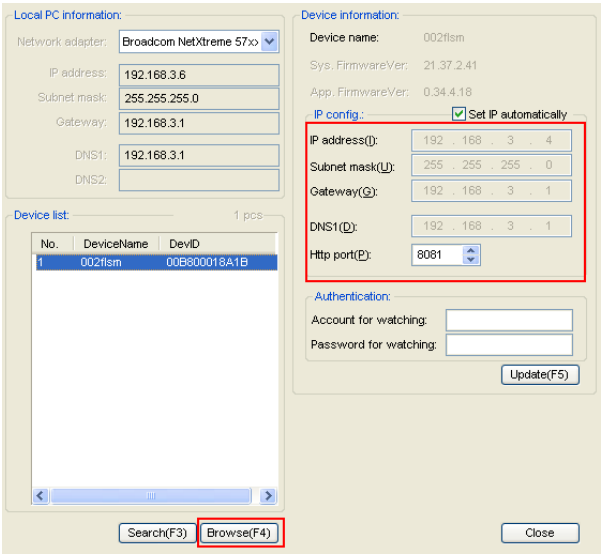
Installation

For Windows XP/Vista/7

1. Insert the WIPC302 Resource CD into the CD-ROM drive.
2. Click the Start button on your computer, and then select My Computer.
3. Right click on the D drive (where D: is your CD-ROM drive) then select Explore.
4. Copy and paste WIPC302 Utility into your computer's desktop.
5. To launch the utility double click WIPC302 Utility then click Search (F3)



6. Device List table will automatically be populated. Select your IP camera, and then click **Browse (F4).**



7. This will launch the IP Camera's WEB User Interface. Input **admin** for both username and password then click **OK**.

Connect to 192.168.3.3
The server 192.168.3.3 at ipcamera_00B800018A1B requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

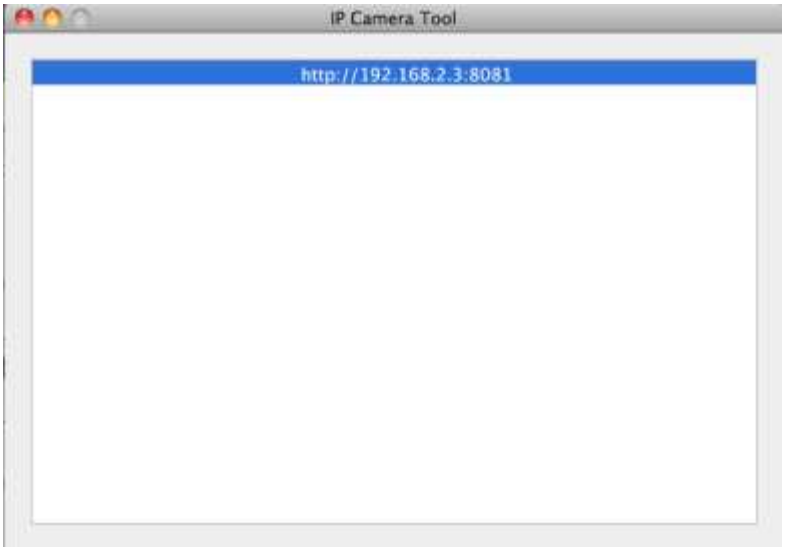
For Mac OSX

1. Insert the WIPC302 Resource CD into the CD-ROM drive.
2. Click the Start button on your computer, and then select My Computer.
3. Right click on the D drive (where D: is your CD-ROM drive) then select Explore.
4. Copy and save MAC Search Tool on your computer's desktop.

5. Open the MAC Search Tool folder then double click IP Camera tool

.

6. This will launch the IP Camera tool; ensure that your IP camera and PC are connected to the same router.



7. Double click on the IP Camera's IP address to launch the Web User Interface. Authentication page will appear, input **admin** for both username and password then click **Ok** to login to the Web User Interface.

Connect to 192.168.3.3
The server 192.168.3.3 at ipcamera_00B800018A1B requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

About the Web User Interface

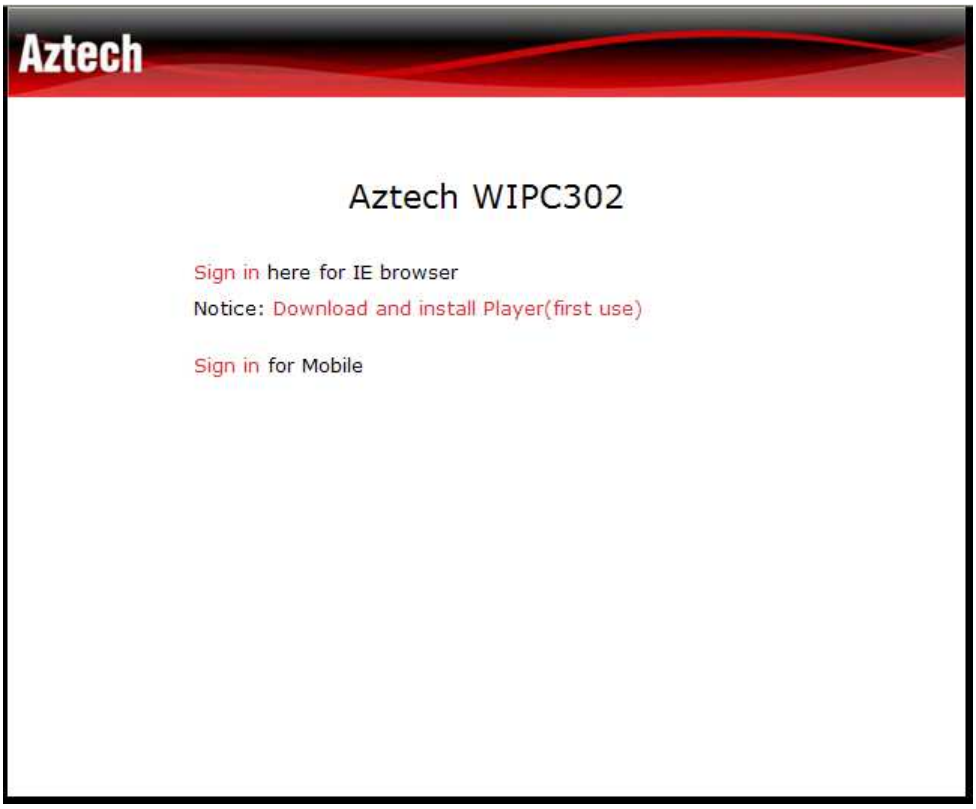
User has two options in accessing the Web User Interface, use the utility or set a static IP address on your computer to launch the Web User Interface to configure the IP camera's settings.

Menus

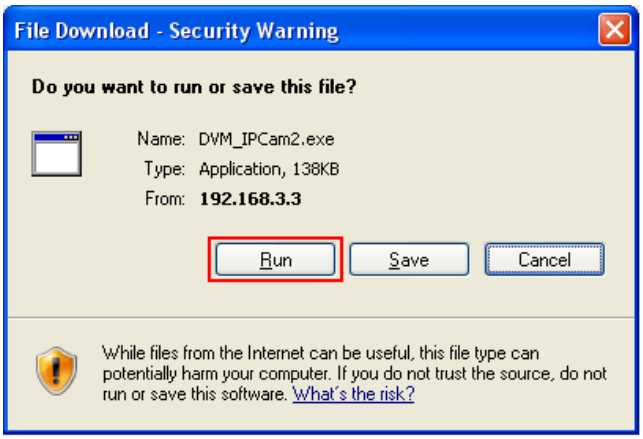
The Web User Interface includes the following menus:

- Home
- Quick Setup
- View
- Network
- Advanced
- Management

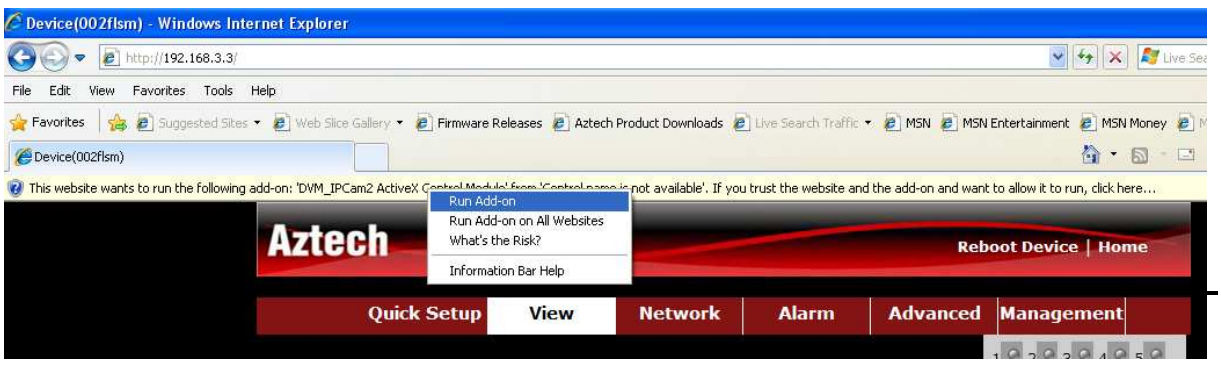
Home



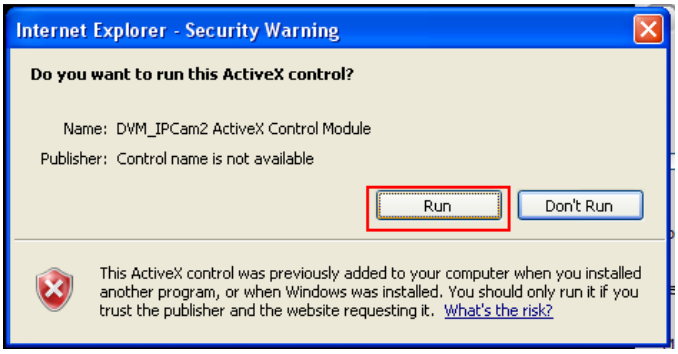
1. For first time use click Download and install Player to view the Video smoothly.


File Download - Security Warning
Do you want to run or save this file?
Name: DVM_IPCam2.exe
Type: Application, 138KB
From: 192.168.3.3
Run
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

2. DVM_IPCam2.exe Message will pop up click Run to install application.


Device(002flsm) - Windows Internet Explorer
http://192.168.3.3/
File Edit View Favorites Tools Help
Favorites
Device(002flsm)
This website wants to run the following add-on: 'DVM_IPCam2 ActiveX Control Module' from 'Control name is not available'. If you trust the website and the add-on and want to allow it to run, click here...
Run Add-on
Run Add-on on All Websites
What's the Risk?
Information Bar Help
Aztech
Reboot Device | Home
Quick Setup
View
Network
Alarm
Advanced
Management

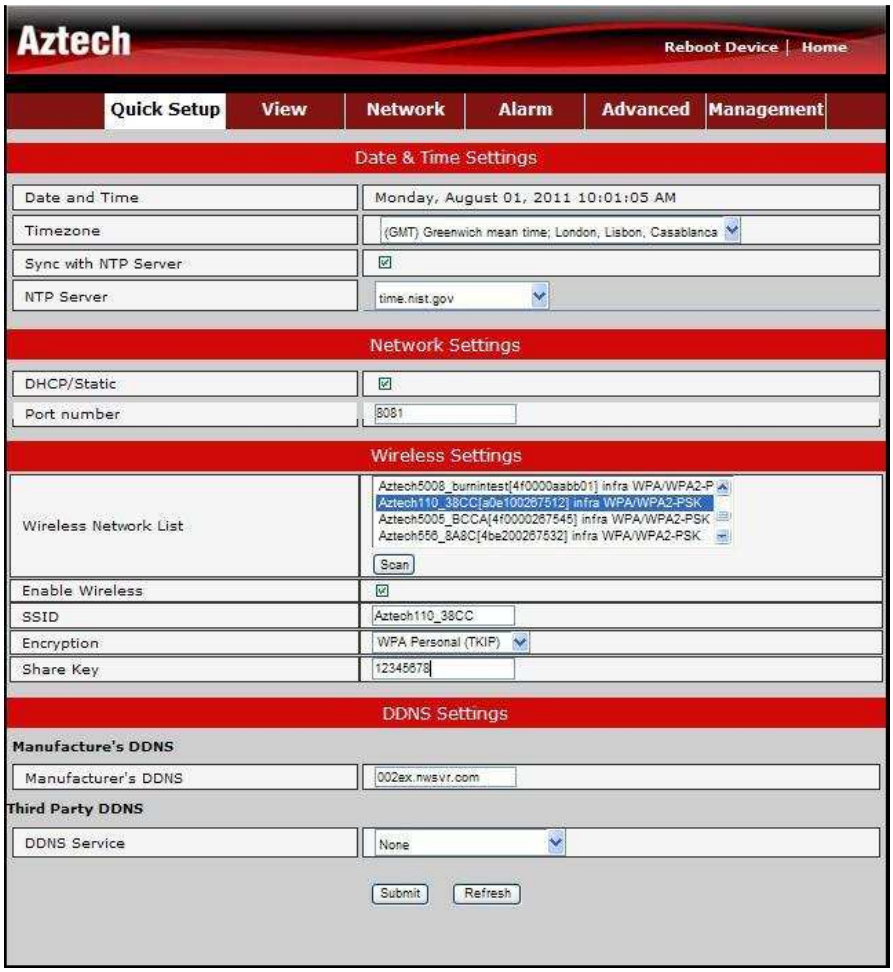
3. Right click on the pop-up message and select Run Add-on


Internet Explorer - Security Warning
Do you want to run this ActiveX control?
Name: DVM_IPCam2 ActiveX Control Module
Publisher: Control name is not available
Run
Don't Run
This ActiveX control was previously added to your computer when you installed another program, or when Windows was installed. You should only run it if you trust the publisher and the website requesting it. What's the risk?

4. DVM_IPCam2 ActiveX Control Module message will appear then click Run.

Quick Setup

Quick Setup will allow user configure the basic settings of the device to be connected to the Internet.



Date and Time Settings

- Select the Timezone that you would like to set on your IP camera.

Network Settings

DHCP/STATIC

- By default your IP camera is set to DHCP wherein it will automatically get an IP address from the DHCP server.
- Uncheck the box to set Static IP address for the IP camera.

Port Number

- Input the port number that you would like to use for the IP camera (It is recommended to use the default port number as some router is using port 80).

Wireless Settings

- Click Scan for the IP camera to search all the available Wireless Access Point.
- Select your Wireless Access Point then input the password on the required field.

DDNS Settings

- You may use the default Manufacturer's DDNS for remote access into your IP camera or you can select the Third party DDNS.
- In selecting a Third party DDNS, it is required to have an active DDNS account for you to access the IP camera via the Internet.

Once you have completed the required information click Submit for the settings to take effect.

Note: It is required to configure **Port Forwarding** on your router for you to access the IP camera via Internet.

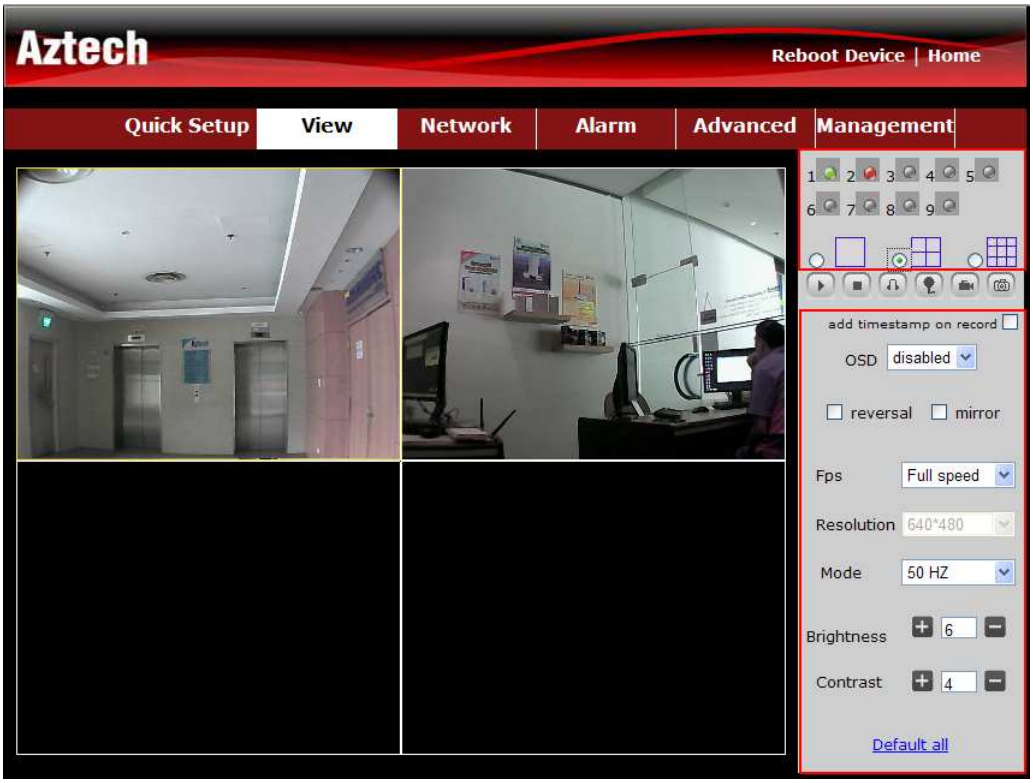
When using the Manufacturer's DDNS do not include the port number when accessing the IP camera (example: http://WIPCxxxxxx.nwsvr.com where xxxxxx is unique for every device).

In using a Third Party DDNS it is required that you have an active DDNS account for you to access the IP camera via the Internet else use the Manufacturer's DDNS. You may refer to the Third Party DDNS server on How to register and create an account.

Check on the **Frequently Asked Questions** on how to access the IP camera on a smart phone and configure port forwarding on some routers.

View

This section allows user to monitor and capture live videos.



Play

- Press this to start Live Video.

Stop

- Press this to stop Live Video.

Audio

- Press this to enable Audio and allows you to hear the sound coming from the live video.
- Press this to disable Audio.

Microphone

- Press this to enable Microphone and allows you to transmit voice via the IP camera.

- Press this to disable Microphone

Recording

- Press this to enable Recording.
- Press this to disable and stop Recording.

Snapshot

- Press this to capture a snapshot of the live video.

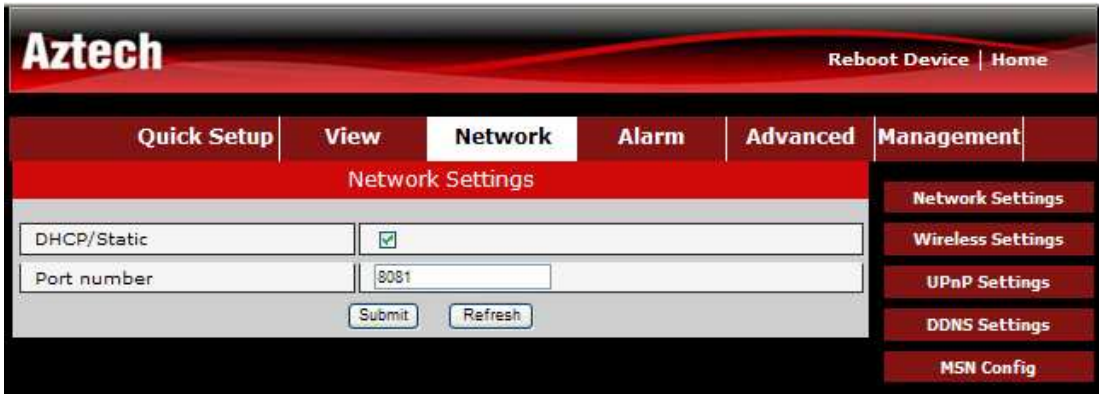
Device Control Monitor

Allows user to view and record video up to 9 devices

- Green device is connected to the network and currently active.
- Red blinking device is connected to the network and Alarm is Active.
- Gray device is not connected to the network
- Add Timestamp on record – displays Time and date during video recording.
- OSD – Allows user to enable the device name and color display.
- Reversal – controls vertical display of the video.
- Mirror – control horizontal display of the video.
- Fps – allows user to set quality of the video. Full speed displays highest video quality.
- Resolution – allows user to choose from different video resolutions 640*480, 320*240, and 160*120.
- Mode – allows user to adjust lighting frequency depending on the environment.
- Brightness – allows user to adjust brightness of the video displayed.
- Contrast – allows user to adjust contrast of the video being displayed.
- Default all – click this to set video display to its factory default.

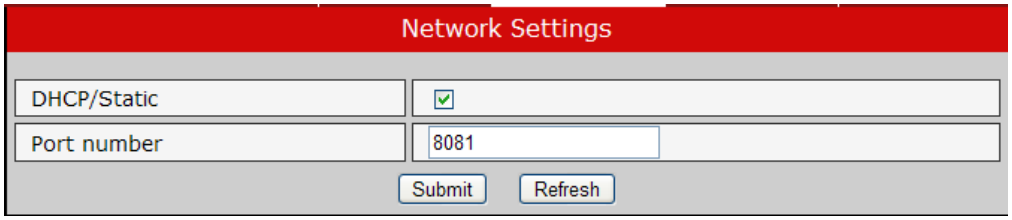
Network

This section allows user to configure Network and Port number settings.

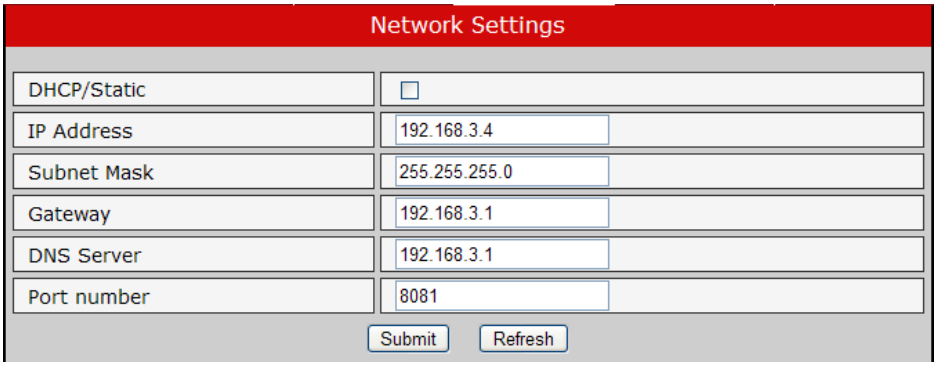


Network Settings

DHCP/Static



- By default your IP camera is set to DHCP wherein it will automatically get an IP address from the DHCP server.



- Uncheck the DHCP/Static box to set Static IP address on the IP camera.
- Static IP – select this option if you have the following information IP address, Subnet Mask, Default Gateway, Primary and Secondary DNS. This information can be obtained from your network administrator.

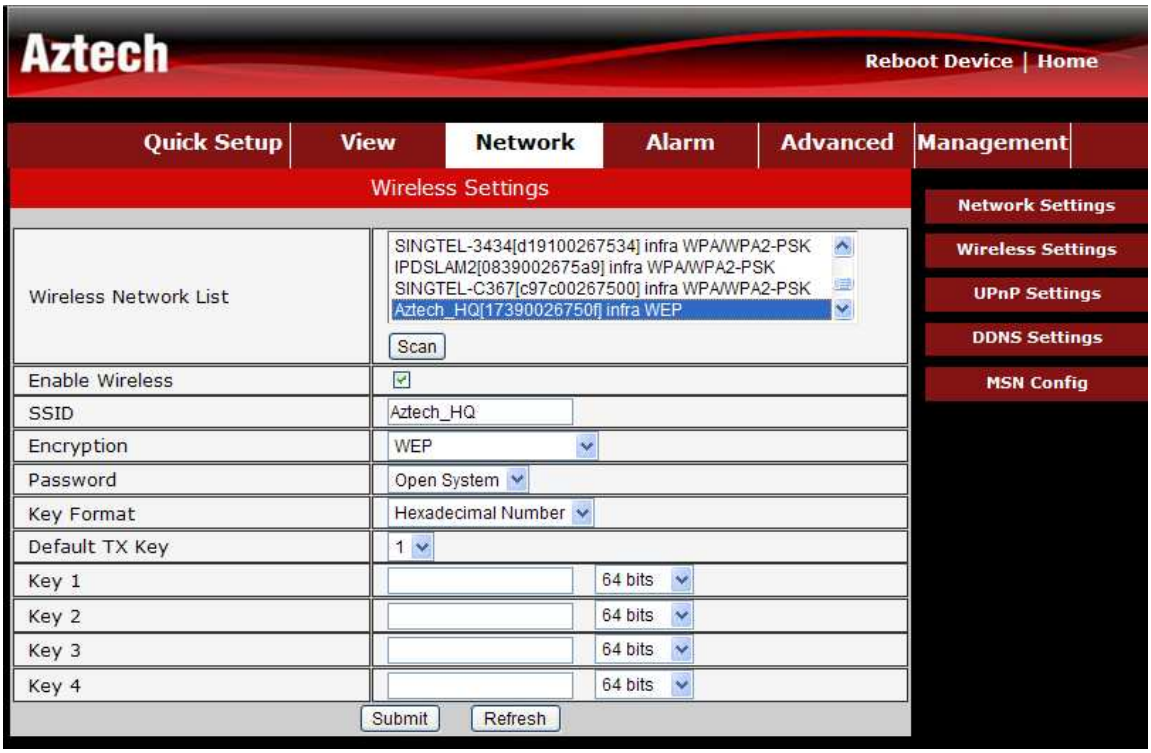
Port Number

- Input the port number that you would like to use for the IP camera (It is recommended to use the default port number as some router is using port 80).

Note: If you have more than 1 IP Camera it is required to use different port number for each camera. Example IP camera-1 port number 8081; IP camera-2 port number 8082

Wireless Settings

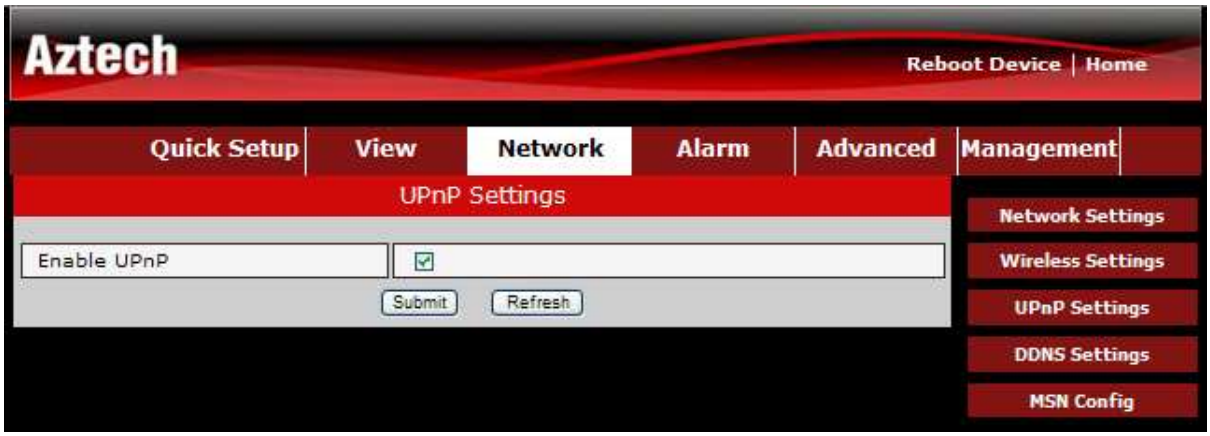
This section allows user to configure the wireless settings of the IP camera.



1. Click Scan for the IP camera to search all the available Wireless Access Point.
2. Select your Wireless Access Point then input the password on the required field then
3. Click Submit for the settings to take effect.

Note: Disconnect the Ethernet cable ONLY after the IP Camera reboots. Your IP Camera will automatically connect to your Wireless Access Point within 2 minutes.

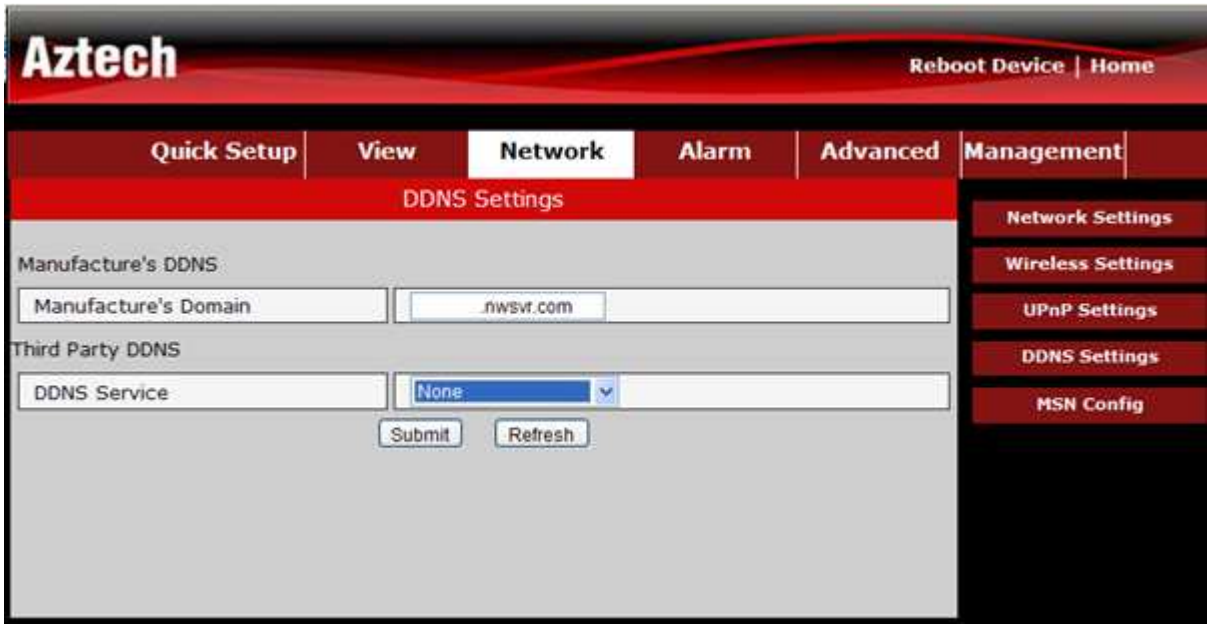
UPnP Settings



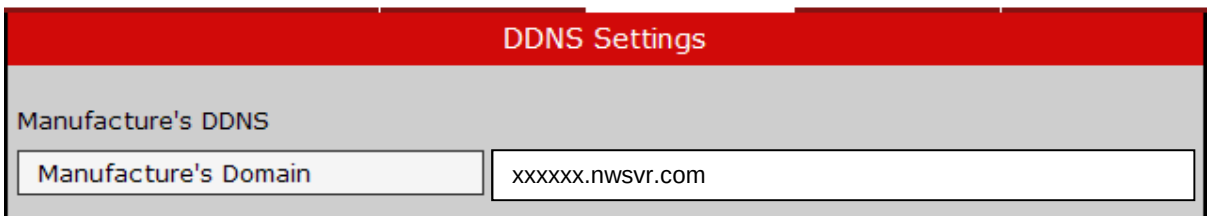
- Enable UPnP – tick the box then click Submit to enable UPnP.

DDNS Settings

This section allows user to configure the DDNS account. User may choose from Manufacturer's DDNS or Third Party DDNS.



Manufacturer's Domain

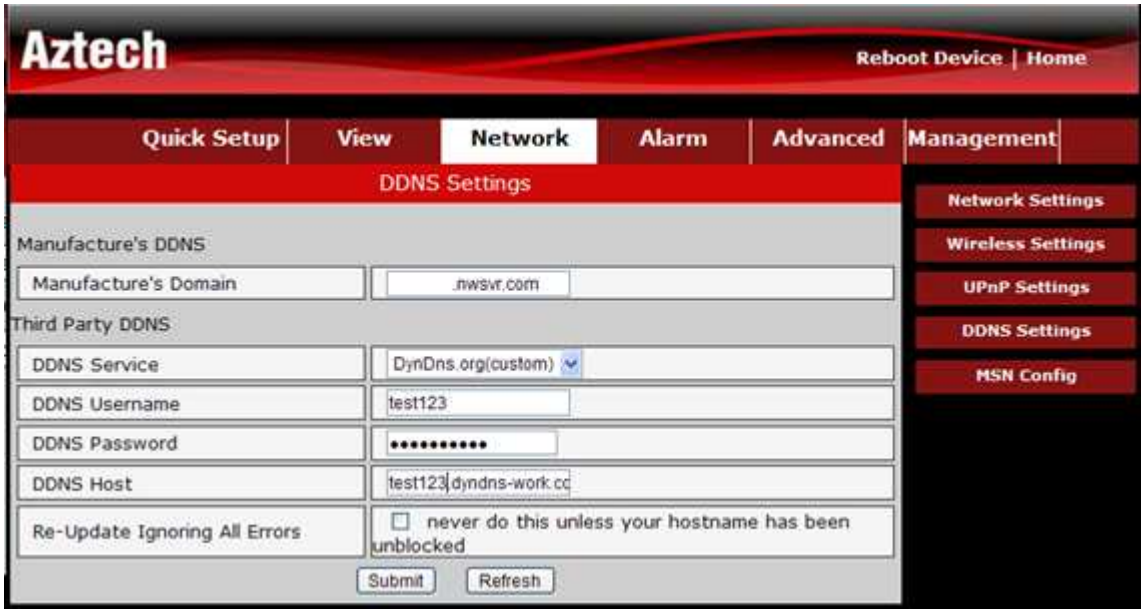


- Use the Manufacturer's DDNS if you don't have an active Third Party DDNS account.

Note: It is required to configure Port Forwarding on your router for you to access the IP camera via Internet.

When using the Manufacturer's DDNS do not include the port number when accessing the IP camera (example: http://xxxxxx.nwsvr.com where xxxxxx is unique for every device).

Third Party DDNS



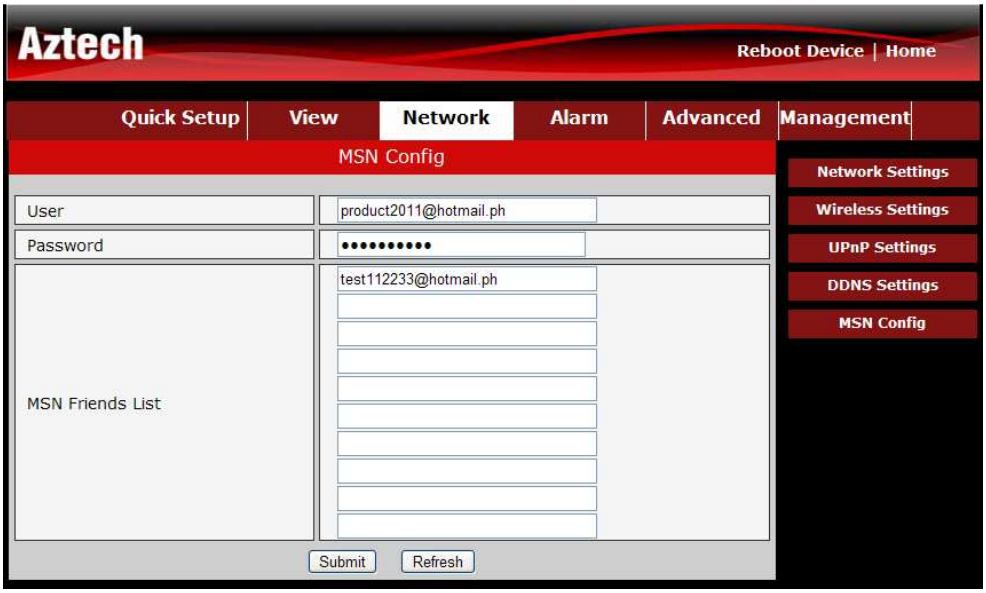
1. DDNS Service – select the DDNS server that you would like to use.
2. DDNS Username – input your DDNS username on the required field.
3. DDNS Password – input your DDNS password on the required field.
4. DDNS Host – input your DDNS hostname on the required field.
5. Click Submit for the settings to take effect.

Note: It is required to configure Port Forwarding on your router for you to access the IP camera via Internet.

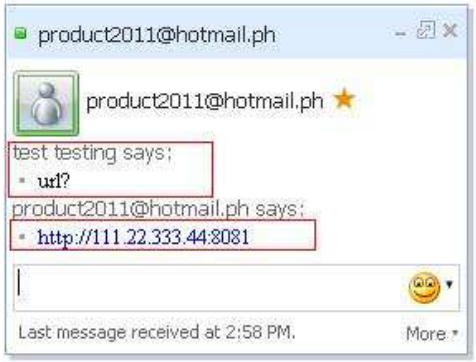
In using a Third Party DDNS it is required that you have an active DDNS account for you to access the IP camera via the Internet. You may refer to the Third Party DDNS server on How to register and create an account.

MSN Config

This section allows the IP camera to send its WAN IP address to the MSN friend List.

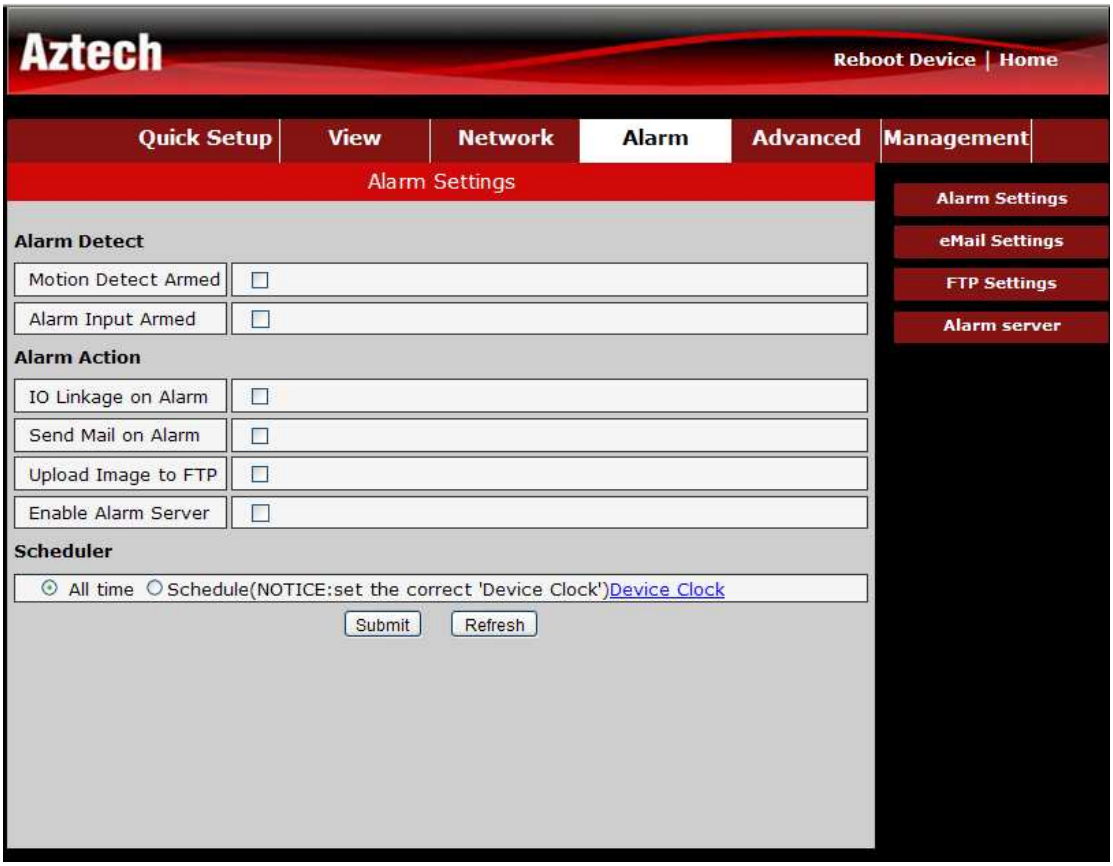


- Input the 1st MSN account under User which will serve as your IP camera's email address.
- Input the 1st MSN account Password on the required field.
- Input your friend's email address on the MSN friends list to allow them to receive the IP camera's WAN IP address
- Using the 2nd MSN account, login to messenger and ensure that the IP camera's email address is added on the contacts.
- Once you see that the IP camera is Online on your messenger send **url?** For the IP camera to reply its WAN IP address.

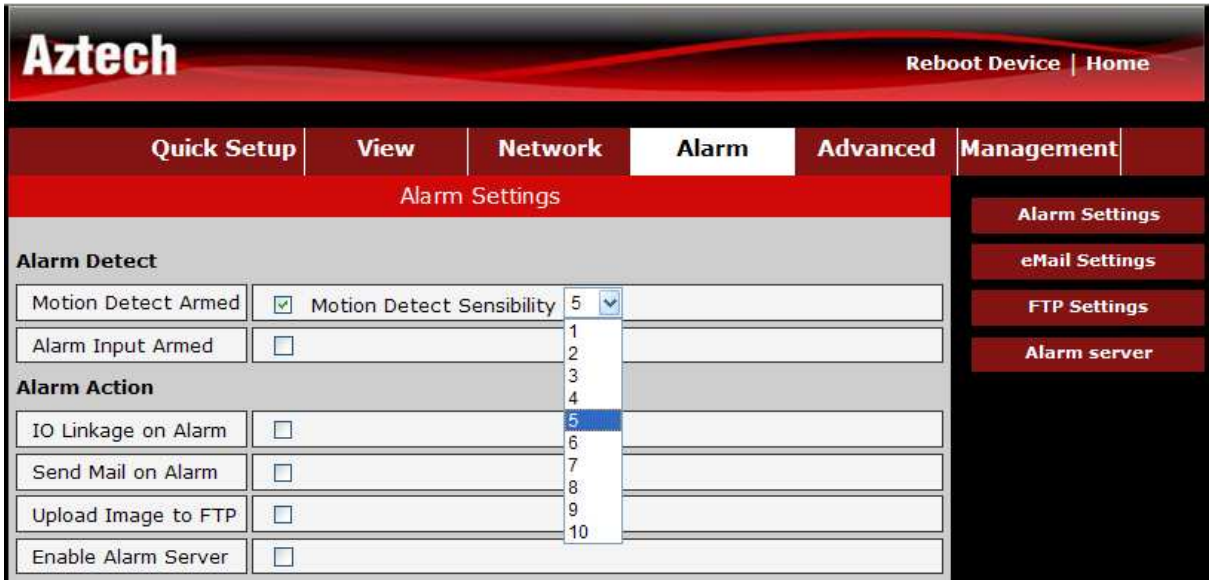


Note: It is required to have 2 MSN account for this feature to work. It is recommended to create an email account for the IP camera.

Alarm



Alarm Settings



Alarm Detect

Alarm Detect enables IP camera to monitor any motion and triggers the alarm.

- Motion Detect Armed – Enables motions detection.
- Motion Detect Sensibility allows user to set motion sensitivity, highest value has the higher sensitivity.

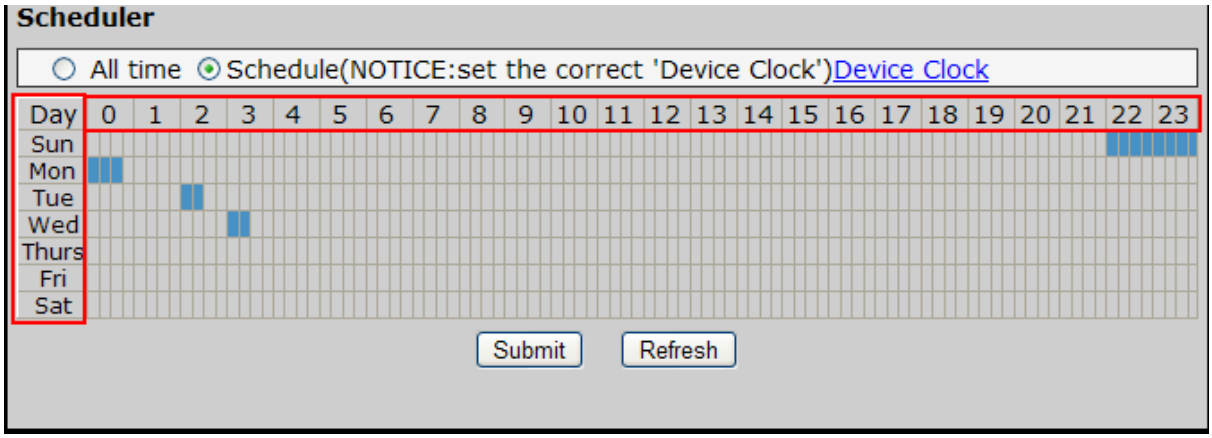
Alarm Action

Once the IP camera detects any motion the device can send an alarm notice. User can select from Email, FTP and Alarm server.

- Send Mail on Alarm IP camera will send alarm info via email.
- Upload Image to FTP IP camera will send snapshot pictures to the FTP server; user can also set the break time between pictures.
- Enable Alarm Server send alarm info to the alarm server

Scheduler

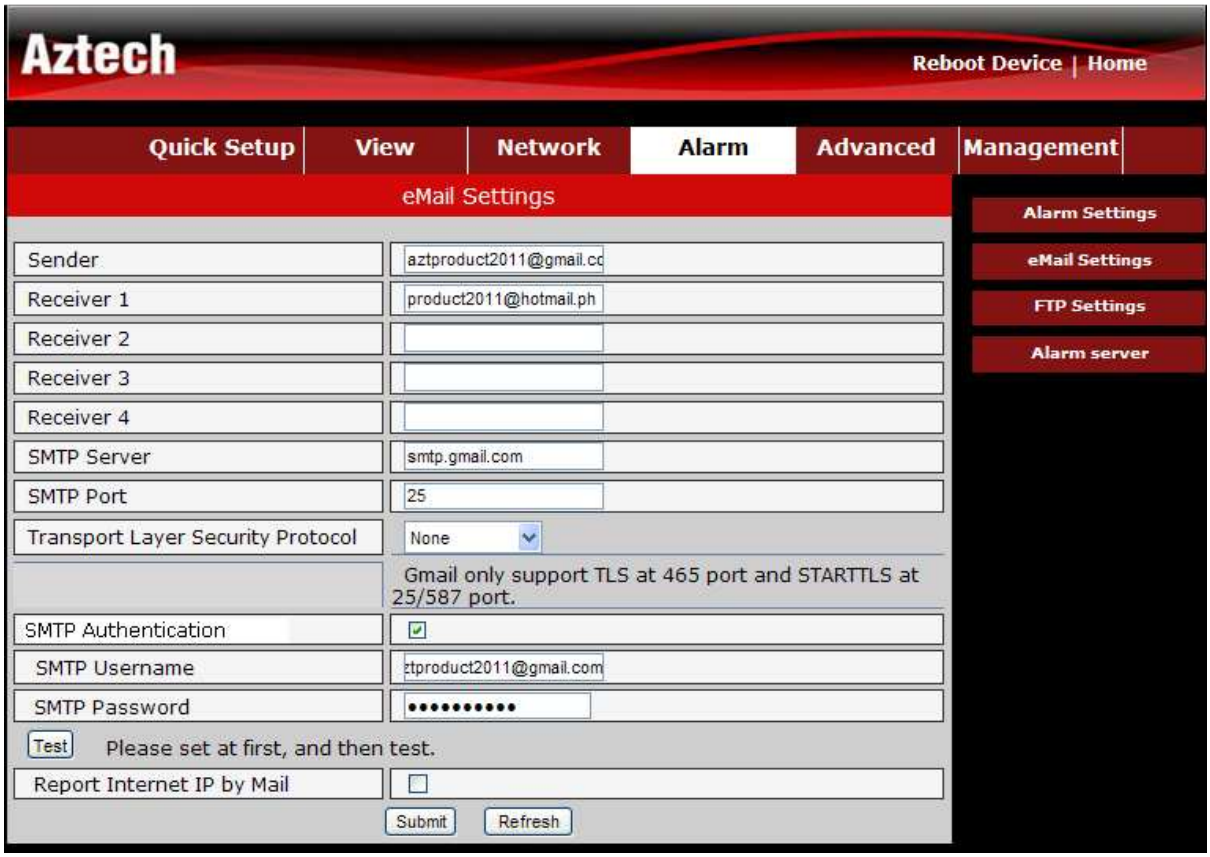
This feature enables the IP camera's Device alarm and triggers it to send notice on the set schedules.



- All Time – select this to for the alarm to be always ON.
- Schedule – select to for a specific day and time to enable the alarm. Boxes correspond to the day and time (Example: Sun 20:00-12:00; Mon 12:00-12:45; Tue 2:00-2:30; Wed 3:00-3:30).

Email

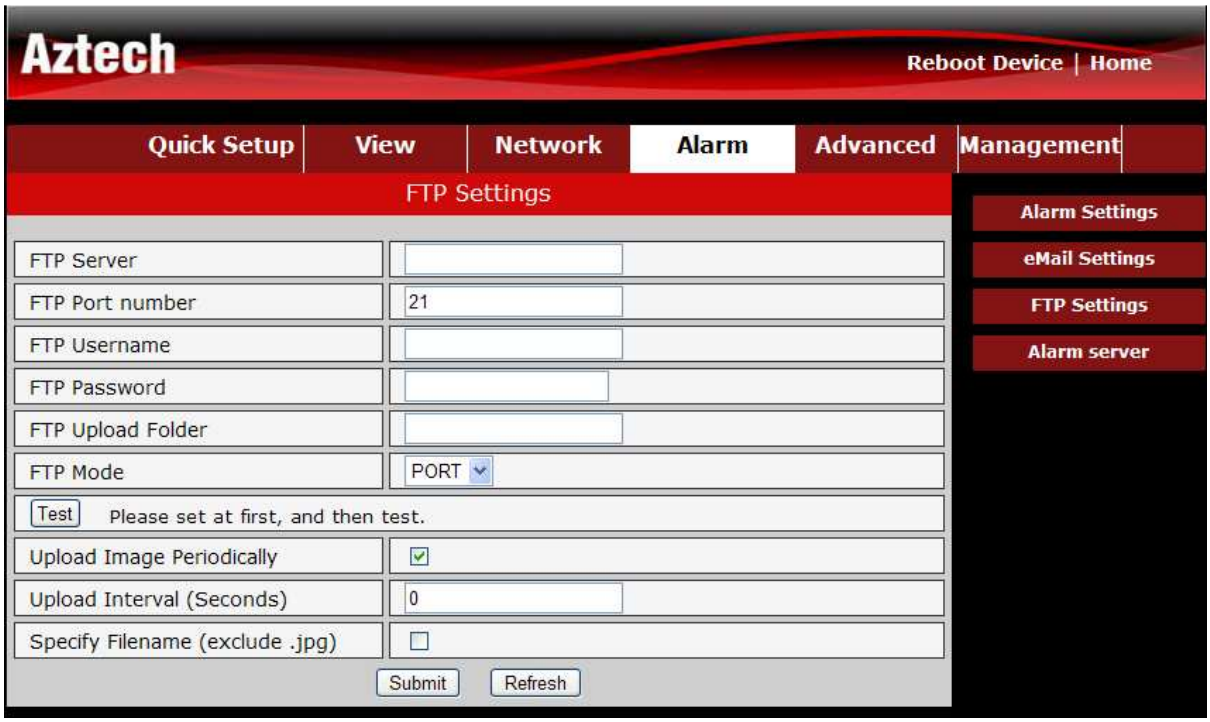
This section allows user to configure the email address for the IP camera to send alarm notice.



1. Sender – input the IP camera's email address on the required field.
2. Receiver 1-4 – input the email addresses of the recipients on the required field.
3. SMTP server – input the SMTP server address on the required field.
4. SMTP Port – input the SMTP server's port number on the required field.
5. SMTP Authentication – tick the box to enable SMTP authentication.
6. SMTP Username – input the sender's email address on the required field.
7. SMTP Password – input the sender's account password on the required field.
8. Click Submit for the settings to take effect.
9. Click Test and then click Management to check the status.

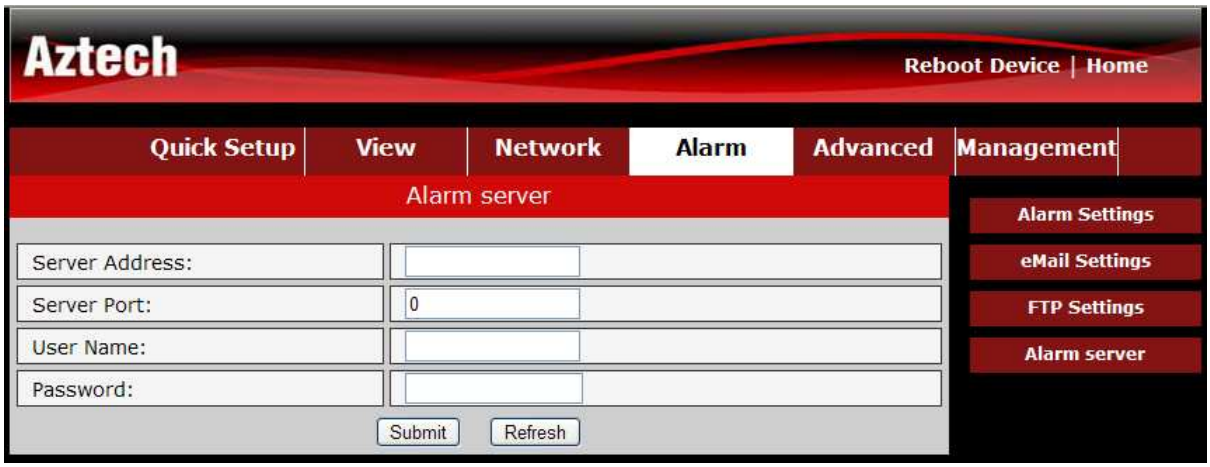
FTP

This section allows user to automatically upload snapshot on the FTP server.



1. FTP Server – input the ftp server's WAN IP address on the required field.
2. FTP Port number – input the FTP server's port number on the required field.
3. FTP Username – input the FTP server's username on the required field.
4. FTP Password – input the FTP server's password on the required field.
5. Upload Image periodically – tick the box to enable the IP camera to upload snapshot on the FTP server.
6. Upload Interval (seconds) – input the interval period of the snapshots to be uploaded on the FTP server.
7. Click Submit for the settings to take effect.

Alarm Server

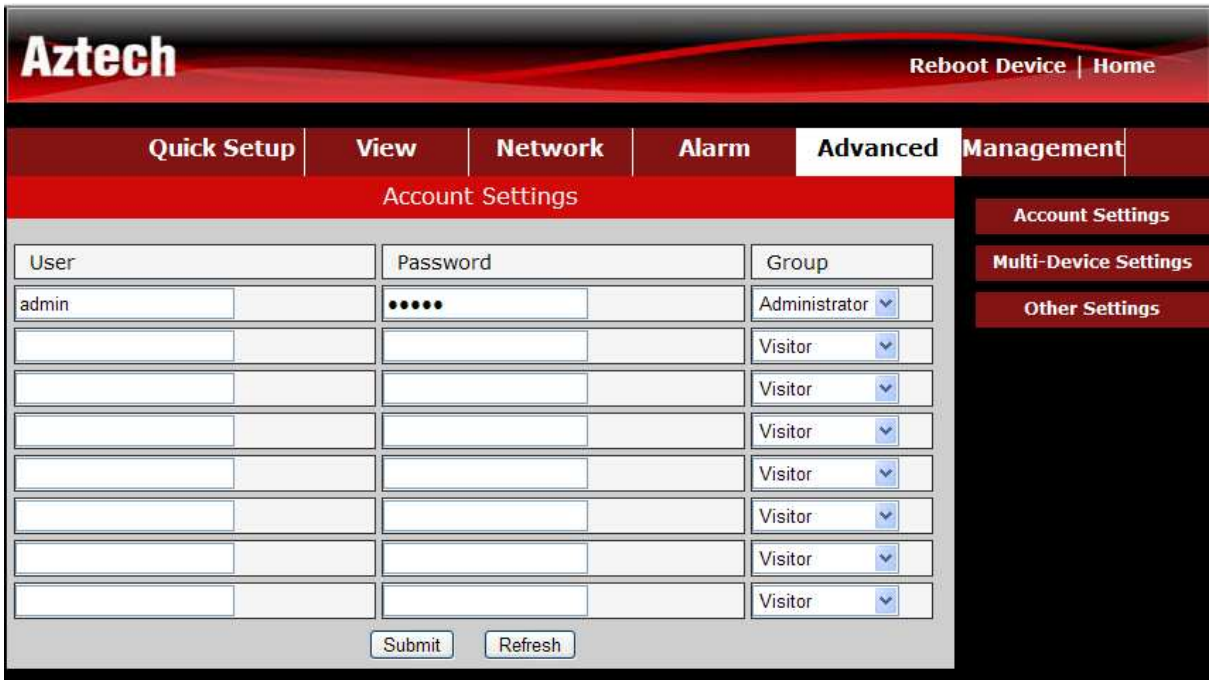


1. Server Address – input the Server's WAN IP address on the required field.
2. Server Port – input the Server's Port number on the required field.
3. Username- input the Server's Username on the required field.
4. Password – input the Server's Password on the required field.
5. Click Submit for the settings to take effect.

Advanced

Account Settings

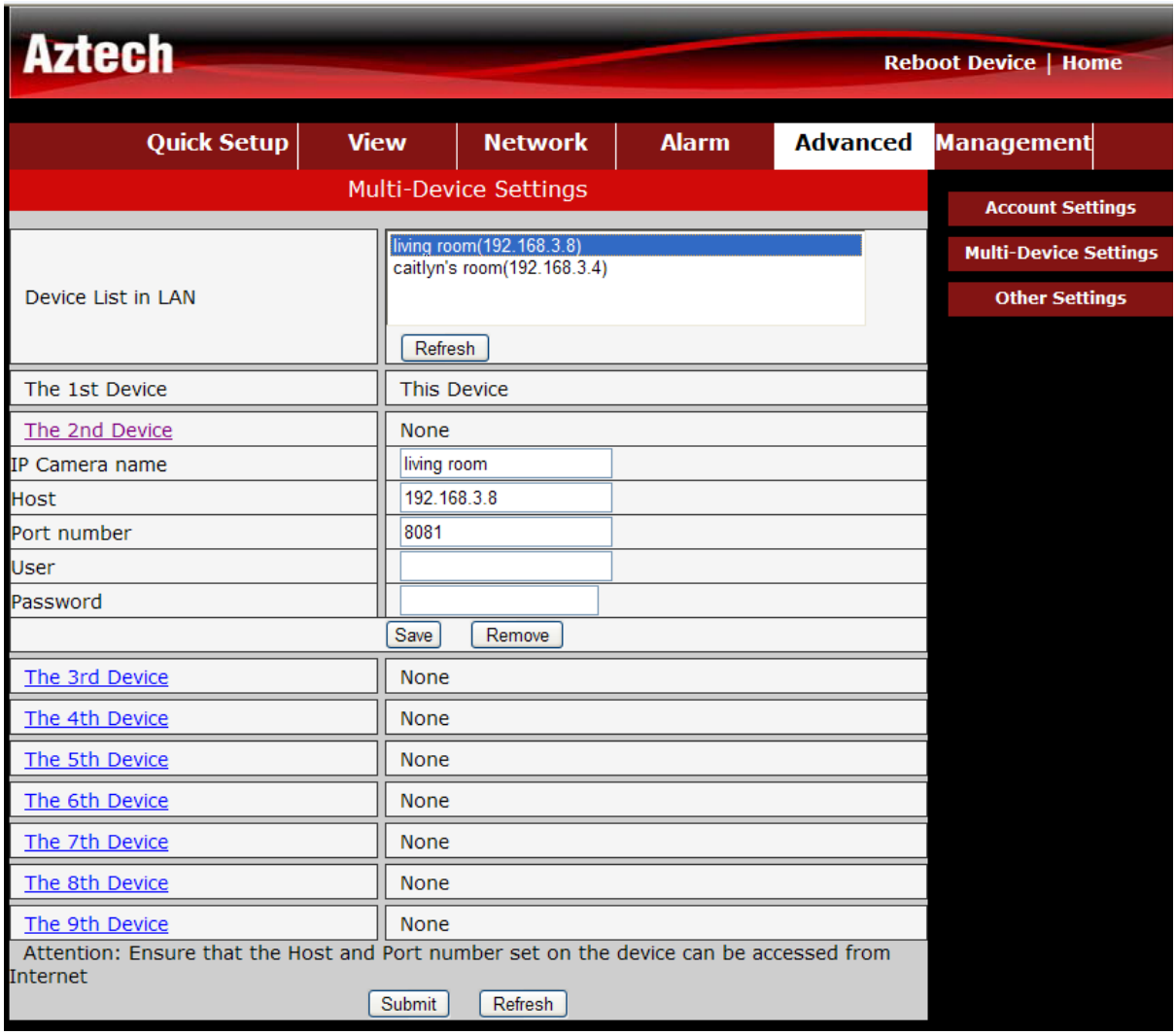
This feature allows you to control the users who will be accessing the device.



- Administrator – user under this account will have a full access on the device.
- Operator – user under this account will only be allowed to change Fps, Resolution, video mode, view, record, talk, hear and capture snapshot of the video
- Visitor – users under this account will only be allowed to view, record, talk, hear and capture snapshot of the video

1. User – input the username that you would like to use to access the WEB User Interface.
2. Password – input the password that you would like to use to access the WEB User Interface.
3. Group – input the account type then click Submit for the settings to take effect.

Multi-Device Settings

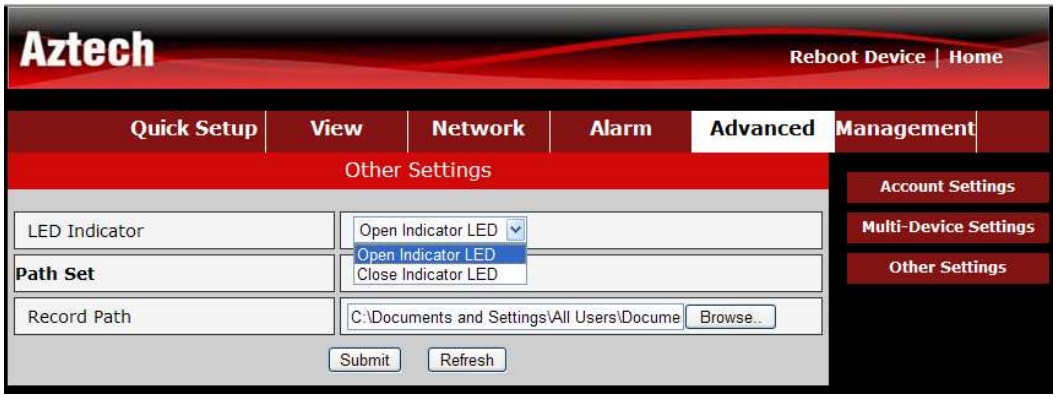


- Device List in LAN displays the entire available IP camera that is connected to your network. Click Refresh update the list of available IP camera.

Adding another IP camera on the list allows user to view multiple videos.

1. Click The 2nd Device then select the IP camera that you would like to add.
2. Input the Username and Password set on the 2nd IP camera.
3. Click Save to save the IP camera's information and then click Submit for the settings to take effect.
4. Click View to view multiple live video (refer to View).

Other Settings

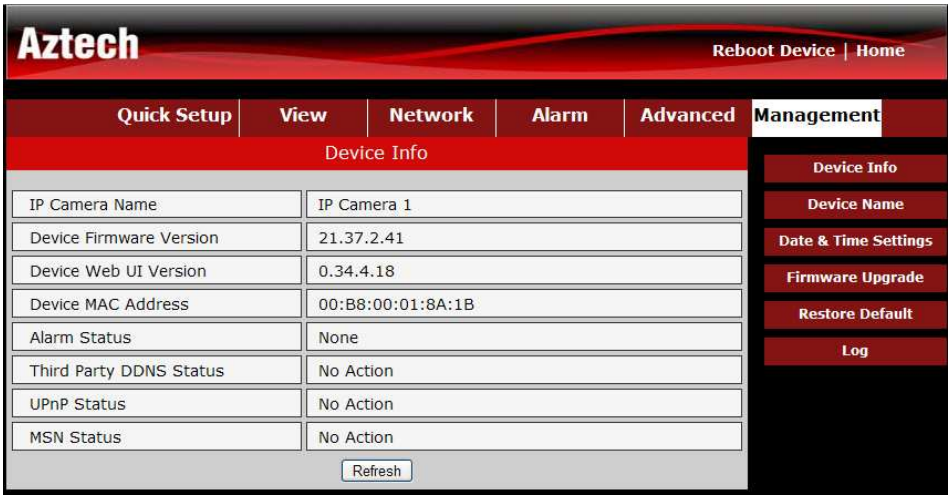


- LED Indicator – enable/disables network LED.
- Record Path – click Browse to set the path for the video to save all recorded files.

Management

Device Info

This section displays a summary of the device status.

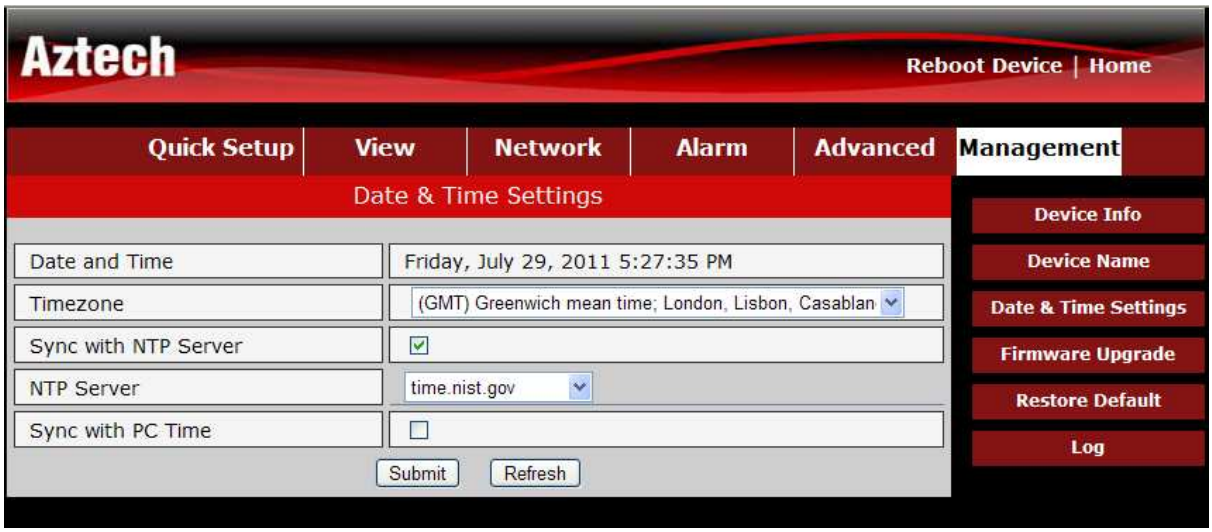


Device Name

- Device Name – allows user to set a name of the IP camera to easily distinguish which device you are viewing.

1. Input the name that you would like to set on the IP camera on the required field.
2. Click Submit for the settings to take effect.

Date and Time Settings



- Timezone – select the Timezone that you would like to set on the IP camera.
- Sync with NTP Server – tick the box for the IP camera to sync to the NTP Server (It is advisable to set the IP camera to Sync with the NTP Server)
- NTP Server – Select the NTP server that you would like to use for the IP camera.
- Sync with PC Time – the IP camera will sync its date and Time with your computer.

Firmware Upgrade

This section allows user to change the current firmware and WEB UI version of the IP camera

1. Click Browse to then select the folder path of the Firmware file.
2. Select the correct firmware file then click Open.
3. Click Submit for the firmware to load into the device.

Note: Do not unplug the Power Adapter or Reboot the device during Firmware Upgrade.

Restore Default

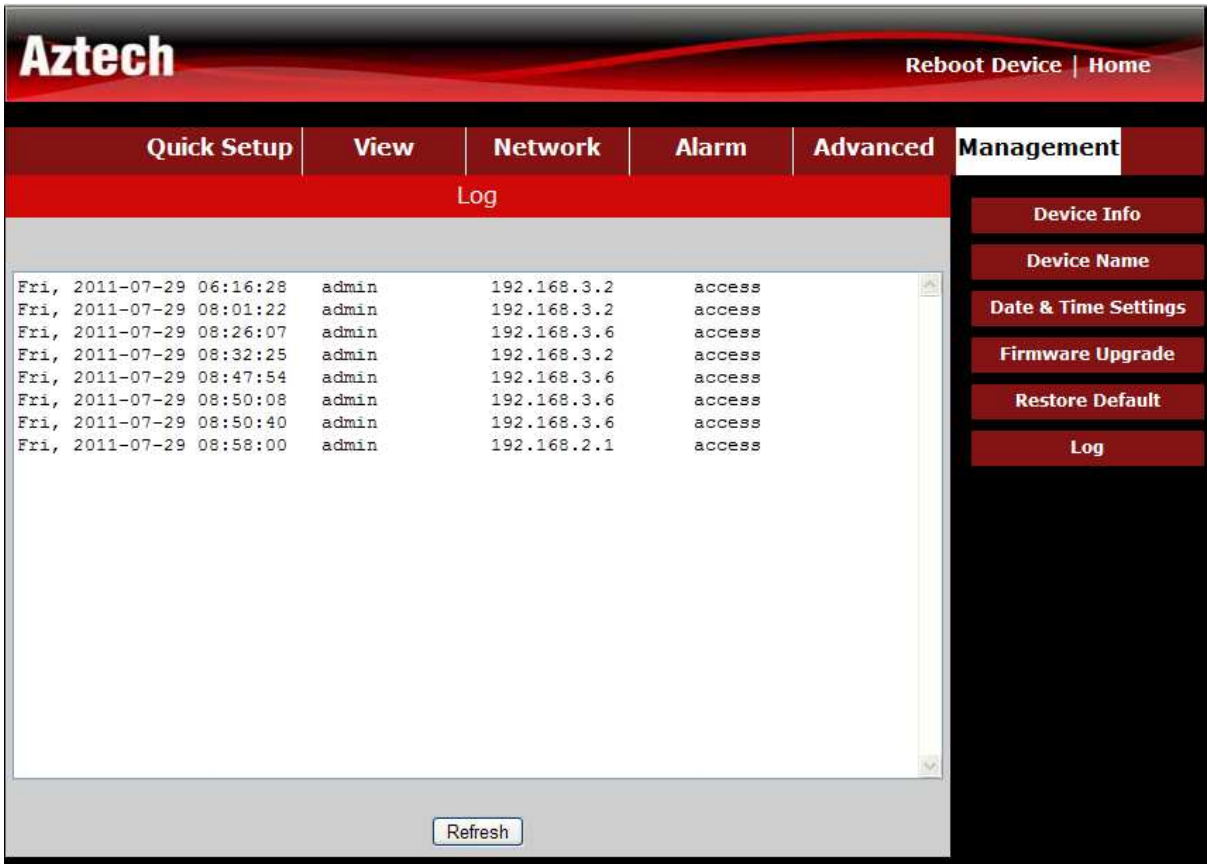
This section allows user to set the IP Camera to its factory Default.

1. Click Restore to Default a pop message will appear.
2. Click OK for the device to go back to its Factory default.

Note: Do not unplug the Power Adapter when the device is Rebooting.

Log

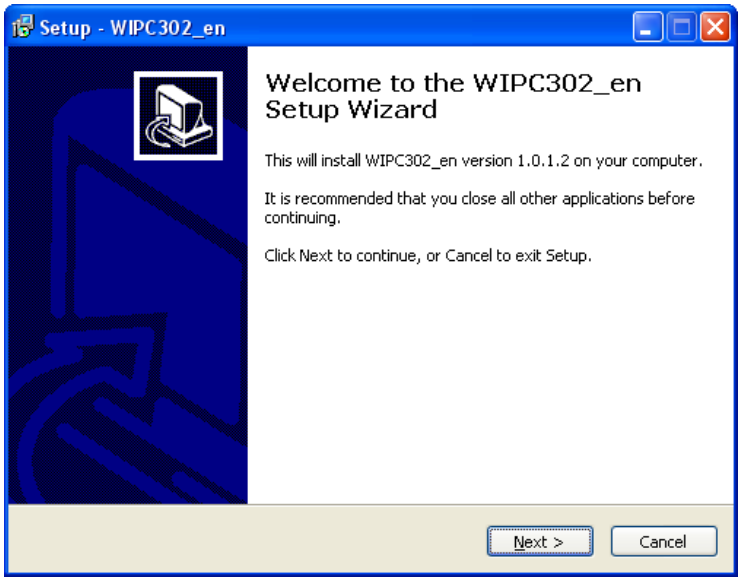
This section allows user to view the log files of the IP camera.



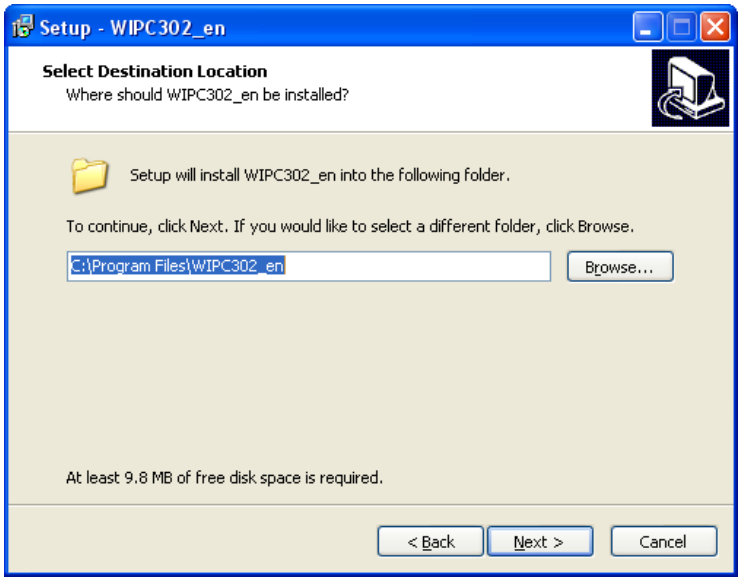
Multiple Device Monitoring System

Installation

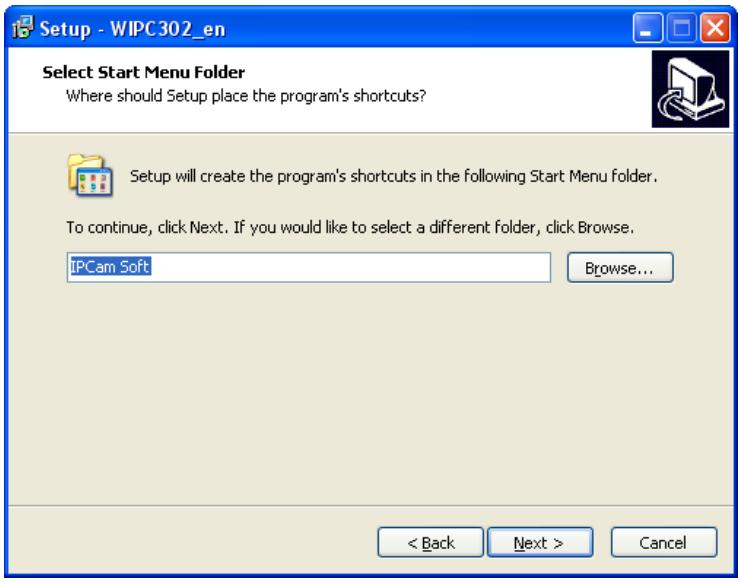
1. Insert the WIPC302 Resource CD into the CD-ROM drive.
2. Click the Start button on your computer, and then select My Computer.
3. Right click on the D drive (where D: is your CD-ROM drive) then select Explore.
4. Double click on WIPC302 Multiple Device Monitoring System.exe to launch the Setup WIPC302_en.


Setup - WIPC302_en
Welcome to the WIPC302_en Setup Wizard
This will install WIPC302_en version 1.0.1.2 on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
Next >
Cancel

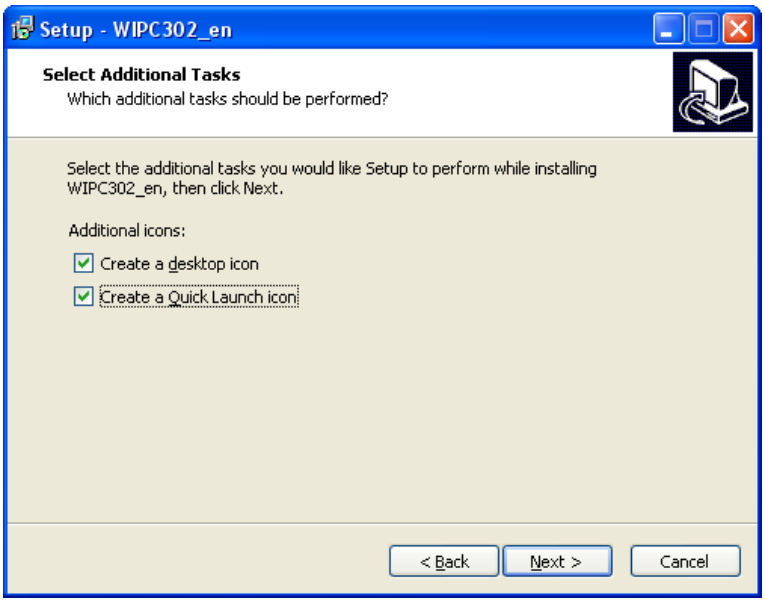
5. Click Next to proceed with the installation.


Setup - WIPC302_en
Select Destination Location
Where should WIPC302_en be installed?
Setup will install WIPC302_en into the following folder.
To continue, click Next. If you would like to select a different folder, click Browse.
C:\Program Files\WIPC302_en
Browse...
At least 9.8 MB of free disk space is required.
< Back
Next >
Cancel

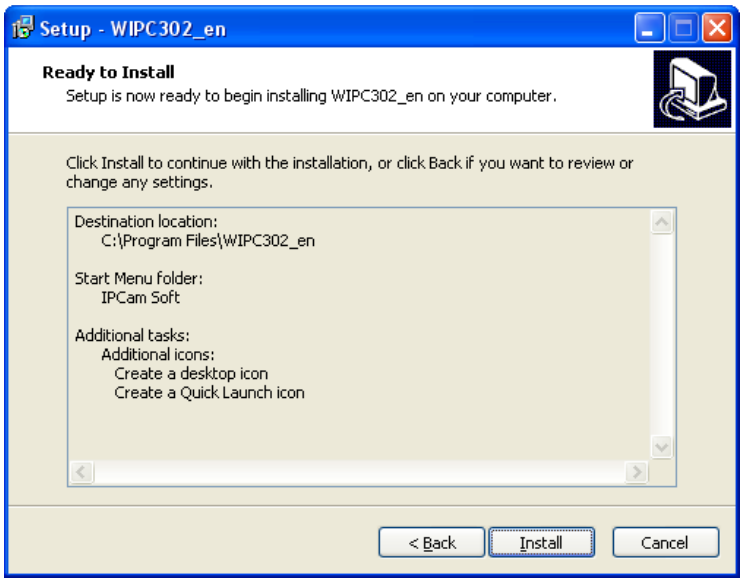
6. Click Next to continue with the installation or click Browse (optional) to change the folder path and save the WIPC302_en file.


Setup - WIPC302_en
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
IPCam Soft
Browse...
< Back
Next >
Cancel

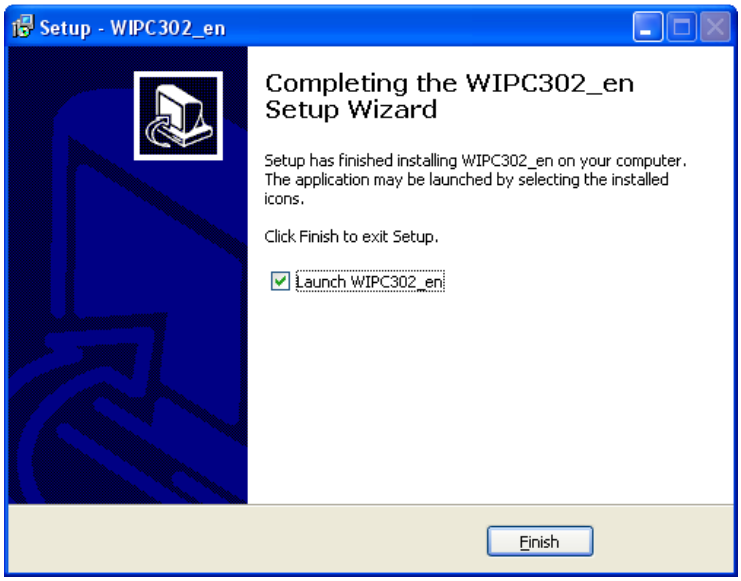
7. Click Next to continue with the installation or click Browse (optional) if you want to change the folder path to save the file.


Setup - WIPC302_en
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing WIPC302_en, then click Next.
Additional icons:
Create a desktop icon
Create a Quick Launch icon
< Back
Next >
Cancel

8. Tick Create a desktop icon and Create a Quick Launch icon then click Next.

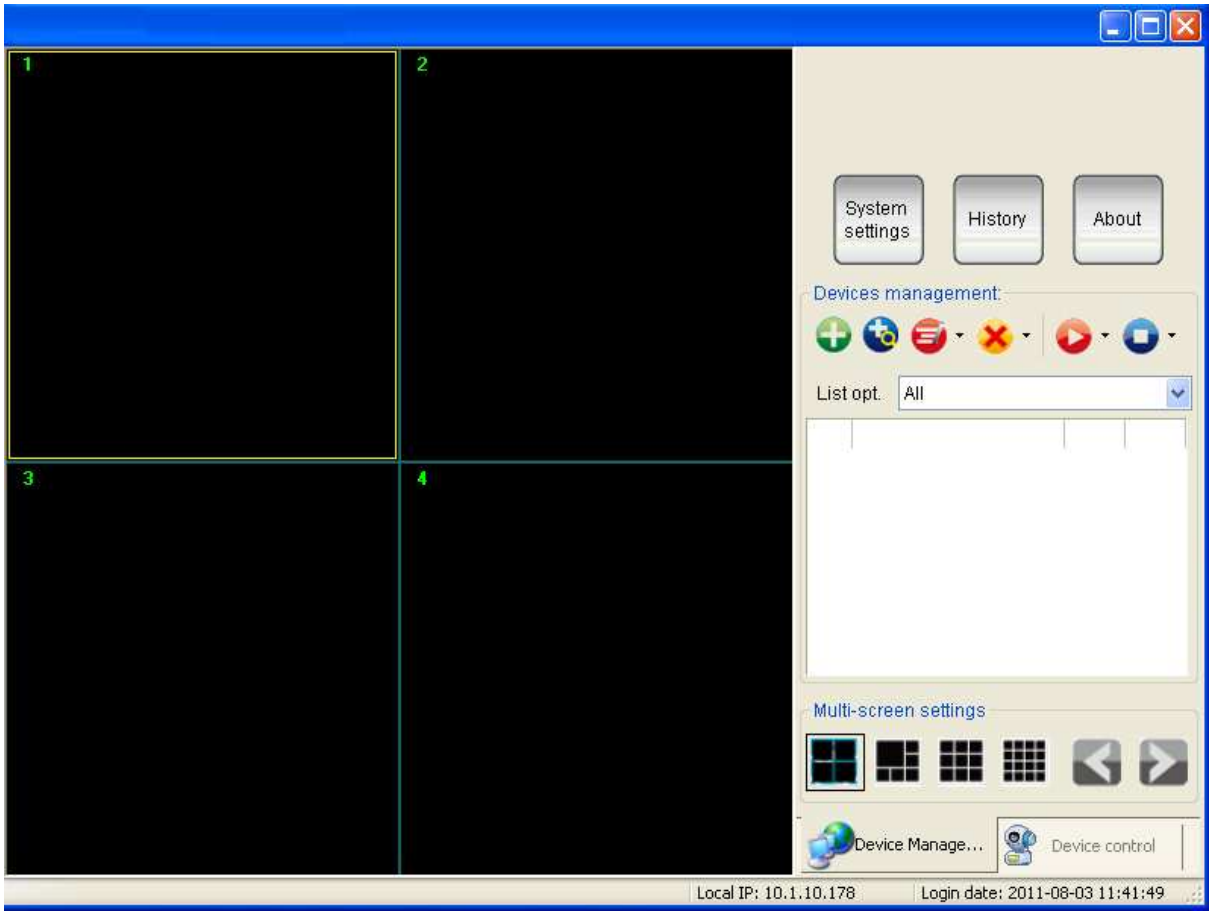

Setup - WIPC302_en
Ready to Install
Setup is now ready to begin installing WIPC302_en on your computer.
Click Install to continue with the installation, or click Back if you want to review or change any settings.
Destination location:
C:\Program Files\WIPC302_en
Start Menu folder:
IPCam Soft
Additional tasks:
Additional icons:
Create a desktop icon
Create a Quick Launch icon
< Back
Install
Cancel

9. Summary page will be displayed click Install to proceed with the installation.

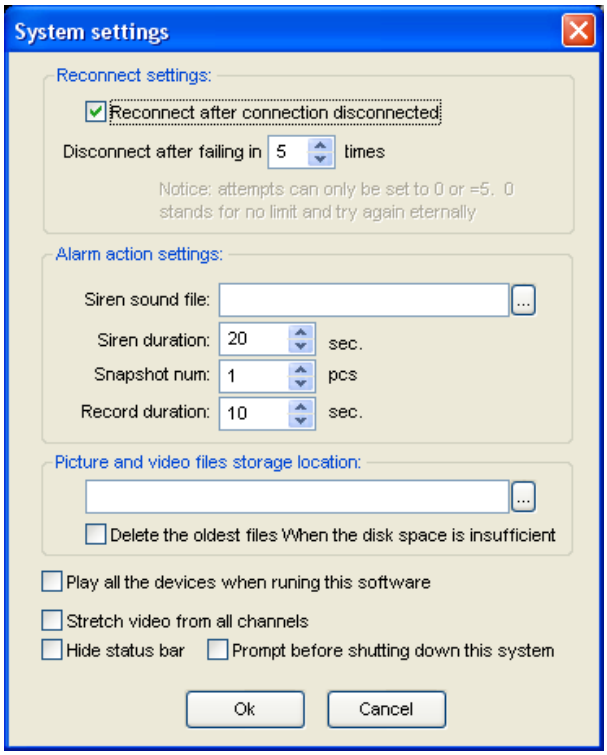

Setup - WIPC302_en
Completing the WIPC302_en Setup Wizard
Setup has finished installing WIPC302_en on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Launch WIPC302_en
Finish

10. Tick Launch then click Finish to complete installation and launch the Multiple Device Monitoring System.

Multiple Device Monitoring System WEB UI



System Settings


System settings
Reconnect settings:
Reconnect after connection disconnected
Disconnect after failing in 5 times
Notice: attempts can only be set to 0 or =5. 0 stands for no limit and try again eternally
Alarm action settings:
Siren sound file:
Siren duration: 20 sec.
Snapshot num: 1 pcs
Record duration: 10 sec.
Picture and video files storage location:
Delete the oldest files When the disk space is insufficient
Play all the devices when runing this software
Stretch video from all channels
Hide status bar
Prompt before shutting down this system
Ok
Cancel

- Reconnect Settings- it allows utility to reconnect to the device. 0 = utility will always attempt to connect to the device.

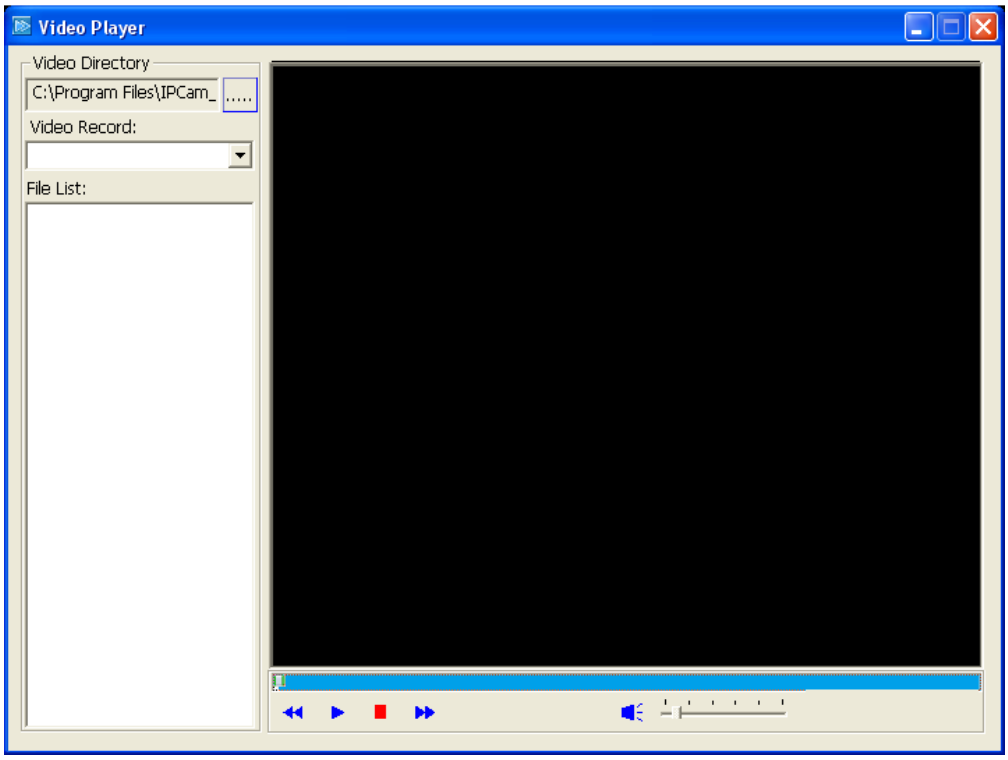
Alarm action settings

- Siren sound file- user may select other sound file (.wav) as siren sound.
- Siren Duration – allows user to set siren duration time. User can set from 20-60 seconds
- Snapshot num – allows user to set the number of snapshot that the camera will capture.
- Record duration – allows user to set duration time for the IP camera to record live video. User can set from 10-30 seconds.

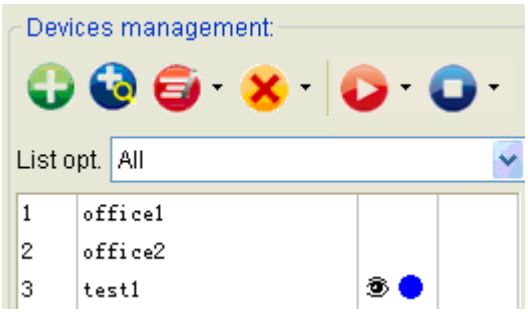
Pictures and video files storage location- user may choose the folder path for the IP camera to store captured images and videos.

History

This section allows user to play recorded videos files.

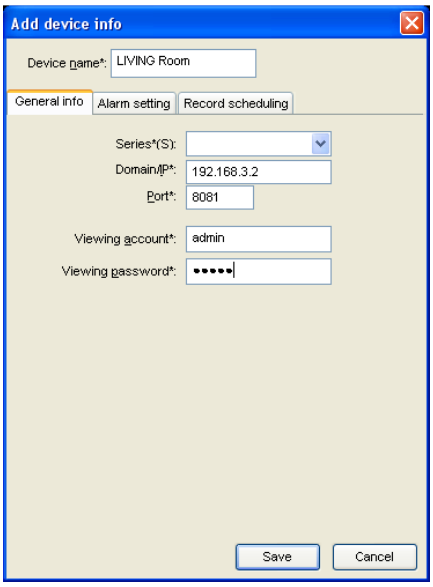


Devices Management

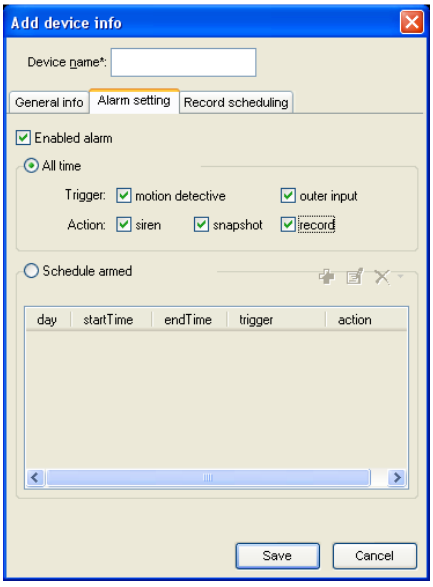


Adding a device

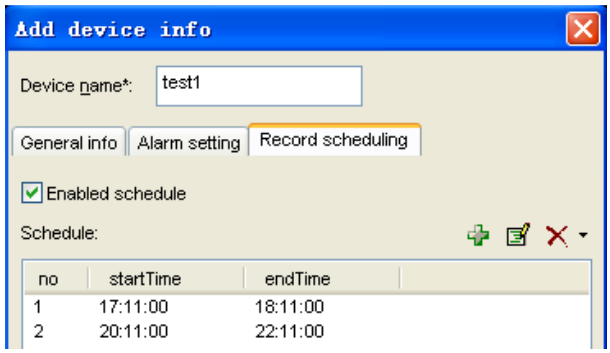
- - click this icon to add an IP camera to be monitored.



- Input the IP camera's information on the required field then click Save for the settings to take effect.



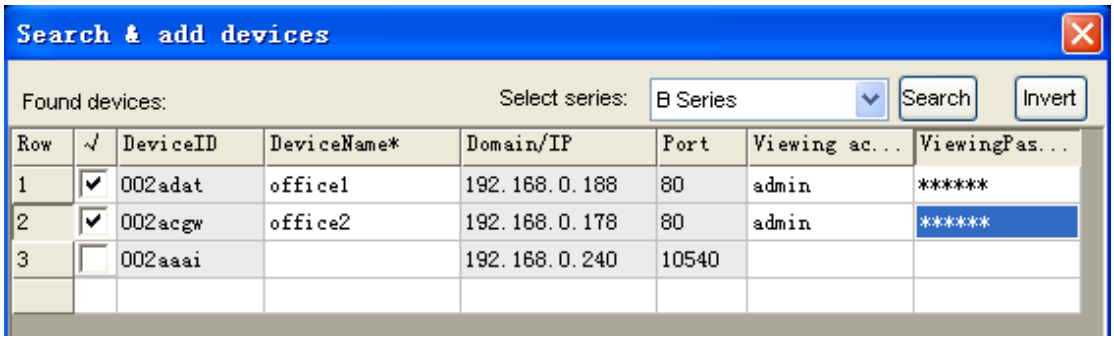
- Tick Enable alarm and tick the commands that the IP camera will do once the alarm is being triggered. Click the Save button for the settings to take effect.



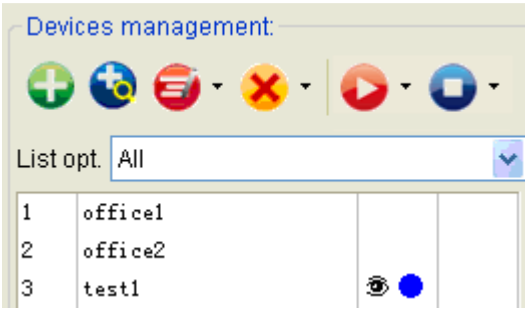
- Record scheduling allows user to set the start and end time for the IP camera to record videos.

Search and add Devices

- - click this icon to search and add more devices.



- - click this icon to edit the IP camera's information. For multiple devices user may choose from the drop down arrow then select the IP camera.
- - click this icon the delete an IP camera on the list. For multiple devices user may choose from the drop down arrow then select the IP camera.
- - click this icon to view the video. For multiple devices user may choose from the drop down arrow then select the IP camera.
- - click this icon to stop the video. For multiple devices user may choose from the drop down arrow then select the IP camera.



- This icon will be displayed shown on the right side of a device, in case alarm is enabled.
- This icon will be displayed on the right side of a device, in case video recording is scheduled.

Frequently Asked Questions

1. **Why I can't access my IP camera when using DDNS?**

- Ensure that the IP camera's IP address and Port number is configured properly on the router.

2. **How do I access my IP camera when using the Manufacturer's DDNS?**

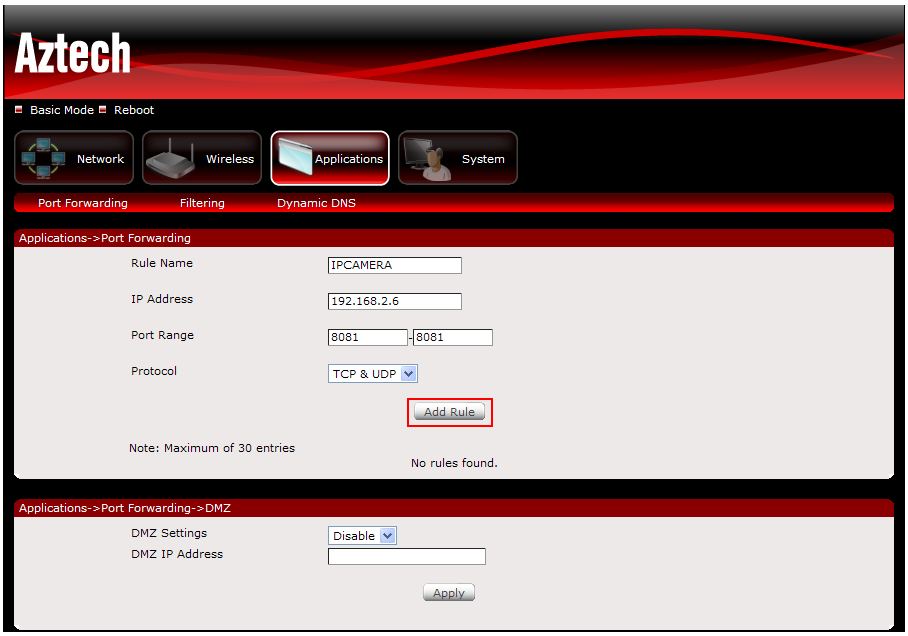
- Ensure that the IP camera's IP address and Port number is configured properly on the router.
- Using another Internet account example your smartphone input the Manufacturer's Domain name on your Web browser http://WIPC001122.nwsvr.com. Do not include the port number when using the Manufacturer's Domain.

3. **How do I configure port forwarding on my router?**

- You may refer to your router's User Manual on How to configure Port Forwarding. Below is an example of Port Forwarding on a HW550-3G.

To configure port forwarding via the Web GUI:

1. Open your browser
2. Type 192.168.2.1 on the address bar
3. Input admin for both username and password fields and click on Login
4. On the top pane, click Advanced Mode to expand the menu and click Applications > Port Forwarding



5. On the Rule Name box input the IP camera's name.
6. On the IP address box input the IP camera's IP address
7. On the Port Range input 8081.
8. Under Protocol set TCP&UDP then click Add rule for the settings to take effect.

4. I can't see any video on the IP camera.

- Ensure that you install the DVM_IPCam2.exe and DVM_IPCam2 ActiveX Control Module to view the video. Click Home then click Download and install Player (first use). Refer to page 17.

5. I can't connect via Wireless.

- Ensure that you have selected the correct Wireless Access Point and input the correct Wireless password.
- Ensure that your router's wireless mode is set to b/g/n.

6. How do I access the IP camera on my phone?

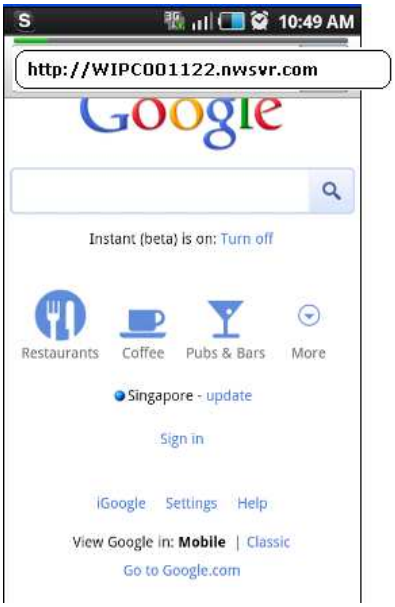
- Ensure that your phone can access the Internet before accessing the IP camera.
- Ensure that the DDNS information was set properly on the IP camera if you are using a Third Party DDNS else use the Manufacturer's DDNS.
- Port Forwarding must be configured on the router refer on your Router's User Manual on how to set Port forwarding.

Below is an example of how you may access the IP camera on a Smart phone.

1. Launch the Internet browser of your phone.

2. Input your IP camera's Manufacturer's DDNS or input your personal DDNS hostname on the address bar.

   For Third Party DDNS it is required to include the IP camera's port number when accessing the video example: http://myhostname.dyndns.org:8081.

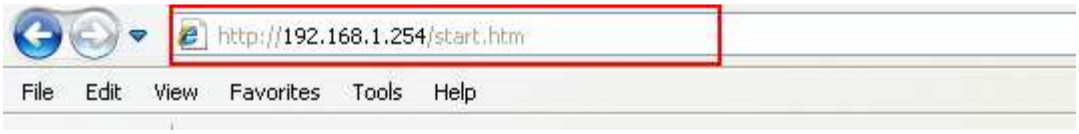


3. This will launch the authentication page, input the username and password that you set on the IP camera then click Sign in.

4. This will launch WIPC302 IP camera's Home page click Sign in for Mobile to access live video.

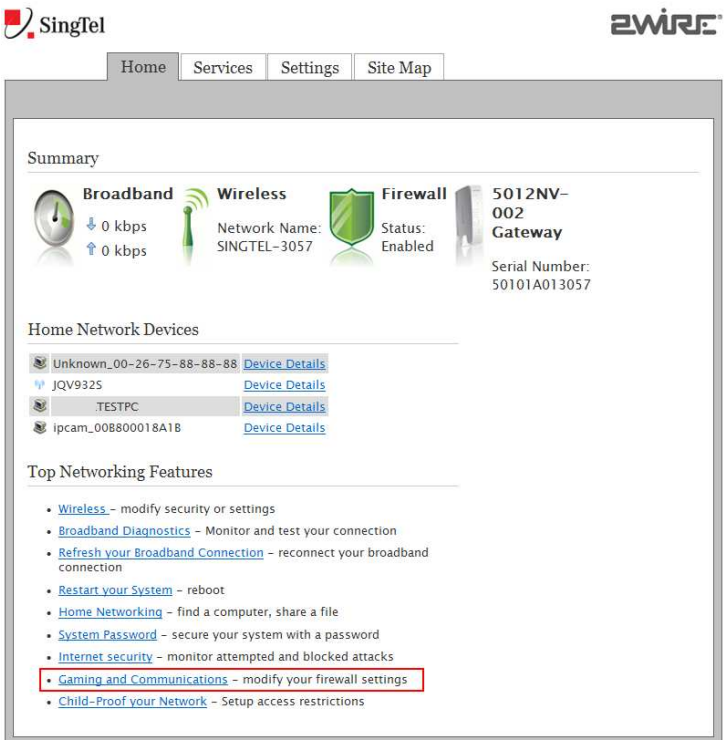
7. How I configure port Forwarding on my 2wire 5012 NV

1. Launch the Internet browser on your computer and input **192.168.1.254**. This will launch your Router's WEB User Interface.

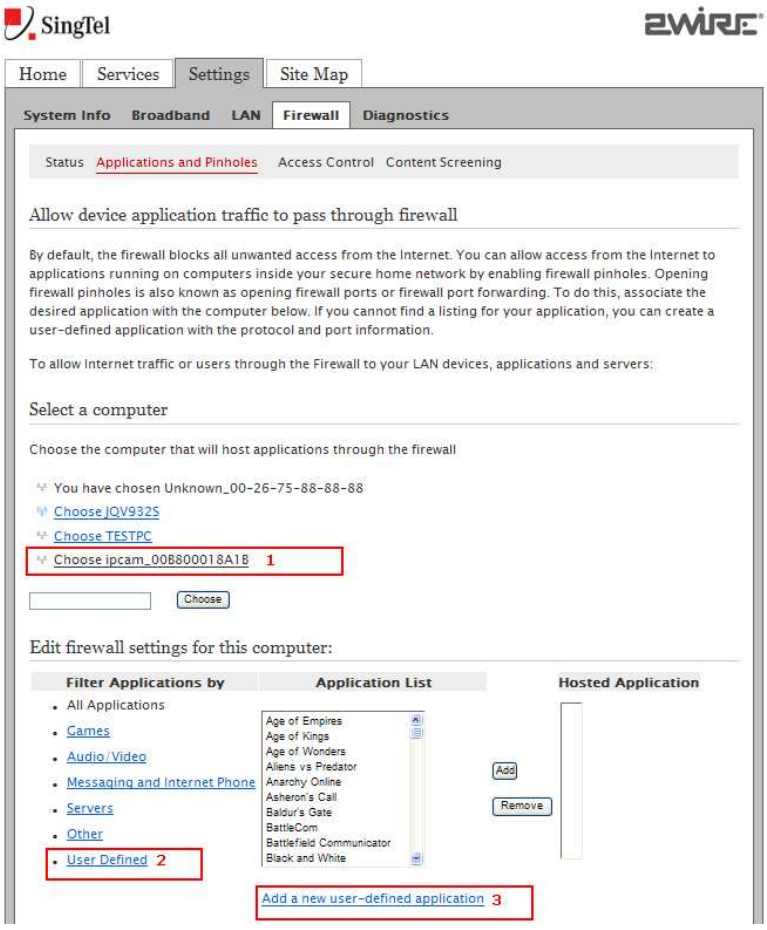


** Note that the login information is based on the default setting of the router.*

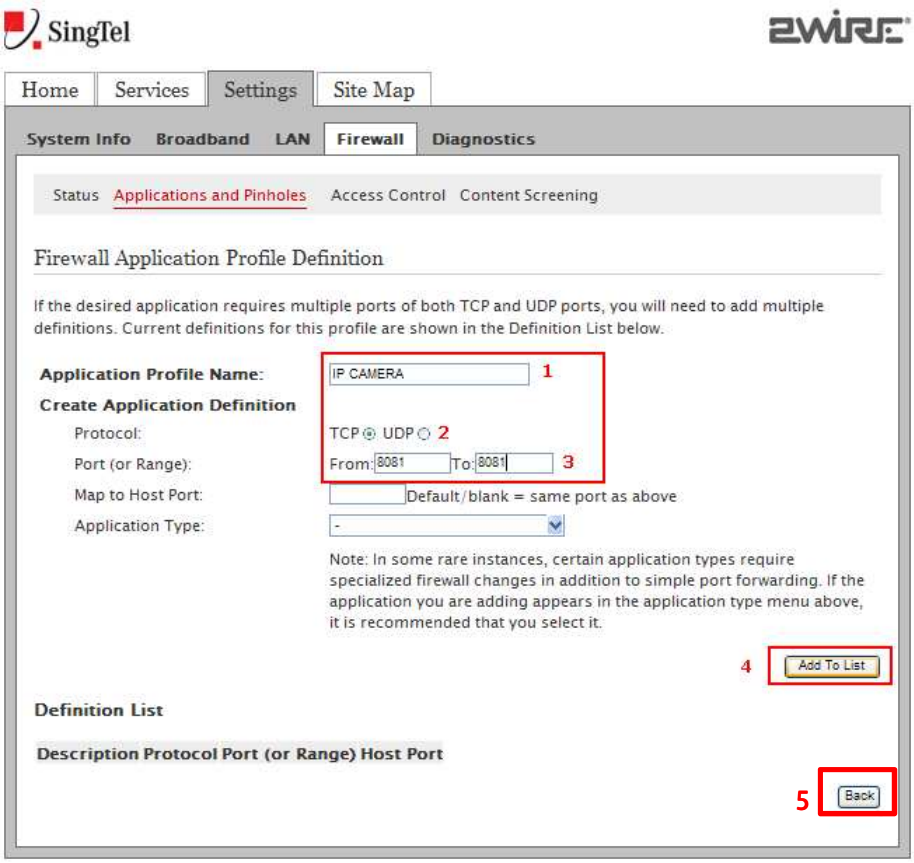
2. Click **Gaming and Communications** to modify the firewall settings of your router.



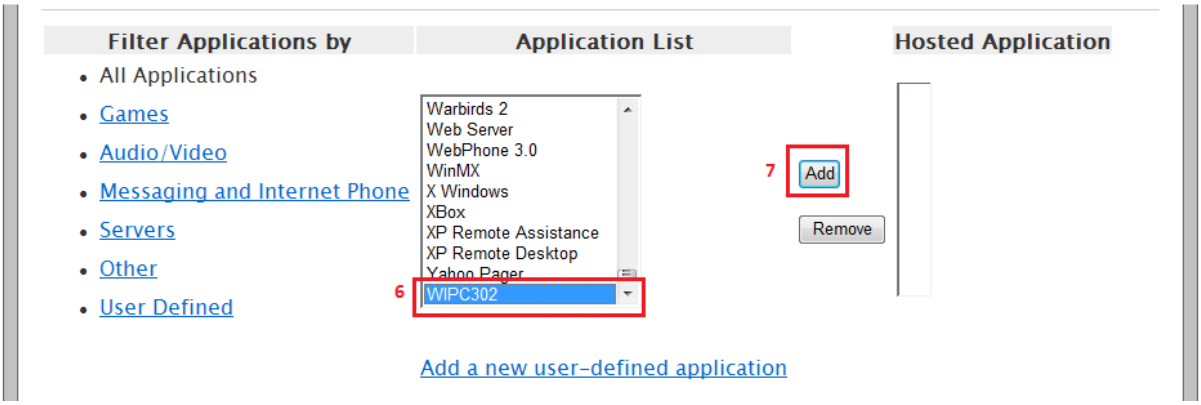
3. Click **WIPC302 IP Camera** then click **User Defined**.


SingTel
2WIRE
Home
Services
Settings
Site Map
System Info
Broadband
LAN
Firewall
Diagnostics
Status
Applications and Pinholes
Access Control
Content Screening
Allow device application traffic to pass through firewall
By default, the firewall blocks all unwanted access from the Internet. You can allow access from the Internet to applications running on computers inside your secure home network by enabling firewall pinholes. Opening firewall pinholes is also known as opening firewall ports or firewall port forwarding. To do this, associate the desired application with the computer below. If you cannot find a listing for your application, you can create a user-defined application with the protocol and port information.
To allow Internet traffic or users through the Firewall to your LAN devices, applications and servers:
Select a computer
Choose the computer that will host applications through the firewall
You have chosen Unknown_00-26-75-88-88-88
Choose JQV932S
Choose TESTPC
Choose ipcam_00B800018A1B 1
Choose
Edit firewall settings for this computer:
Filter Applications by
All Applications
Games
Audio/Video
Messaging and Internet Phone
Servers
Other
User Defined 2
Application List
Age of Empires
Age of Kings
Age of Wonders
Aliens vs Predator
Anarchy Online
Asheron's Call
Baldur's Gate
BattleCom
Battlefield Communicator
Black and White
Add
Remove
Hosted Application
Add a new user-defined application 3

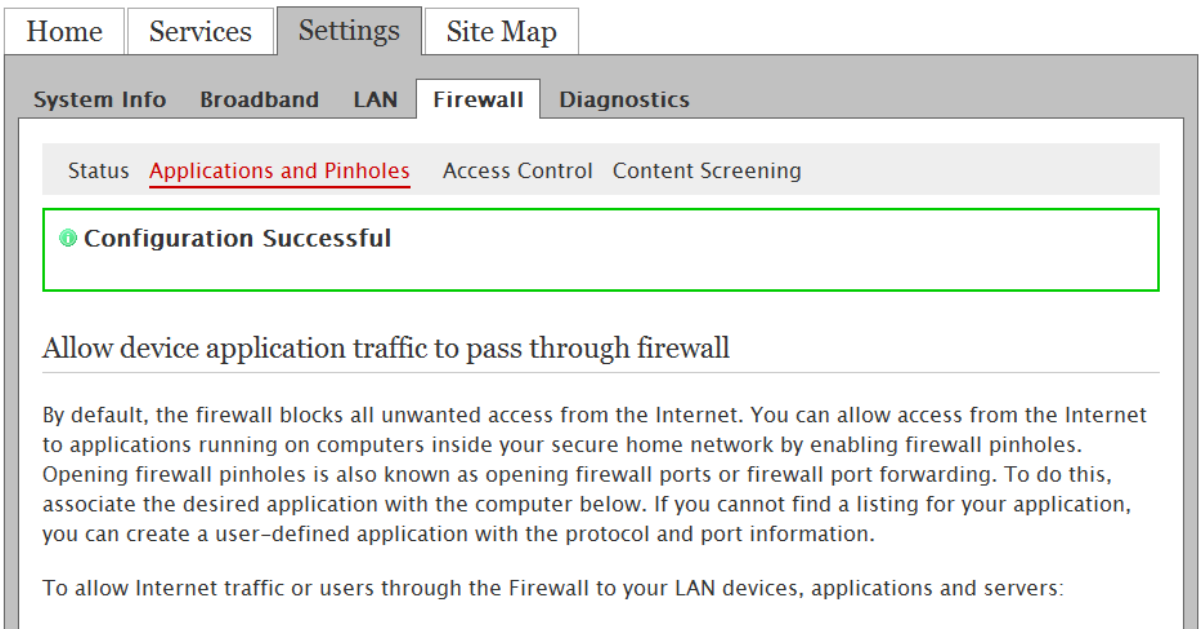
4. Click **Add a new user-defined application** then input the required information. Under **Application Profile Name** input your IP camera's name and select **TCP** under Protocol then input the IP camera's Port number **8081** under Port (or Range) then click **Add to List**. Click **Back** to go back to the Firewall Settings.



5. Under the **Application List** box select the **WIPC302** then click **Add** for the application to be added on the Hosted Application.

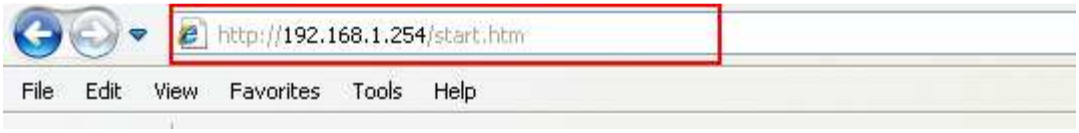


6. Configuration Successful page will be displayed to confirm that the settings have been saved.


Home
Services
Settings
Site Map
System Info
Broadband
LAN
Firewall
Diagnostics
Status
Applications and Pinholes
Access Control
Content Screening
Configuration Successful
Allow device application traffic to pass through firewall
By default, the firewall blocks all unwanted access from the Internet. You can allow access from the Internet to applications running on computers inside your secure home network by enabling firewall pinholes. Opening firewall pinholes is also known as opening firewall ports or firewall port forwarding. To do this, associate the desired application with the computer below. If you cannot find a listing for your application, you can create a user-defined application with the protocol and port information.
To allow Internet traffic or users through the Firewall to your LAN devices, applications and servers:

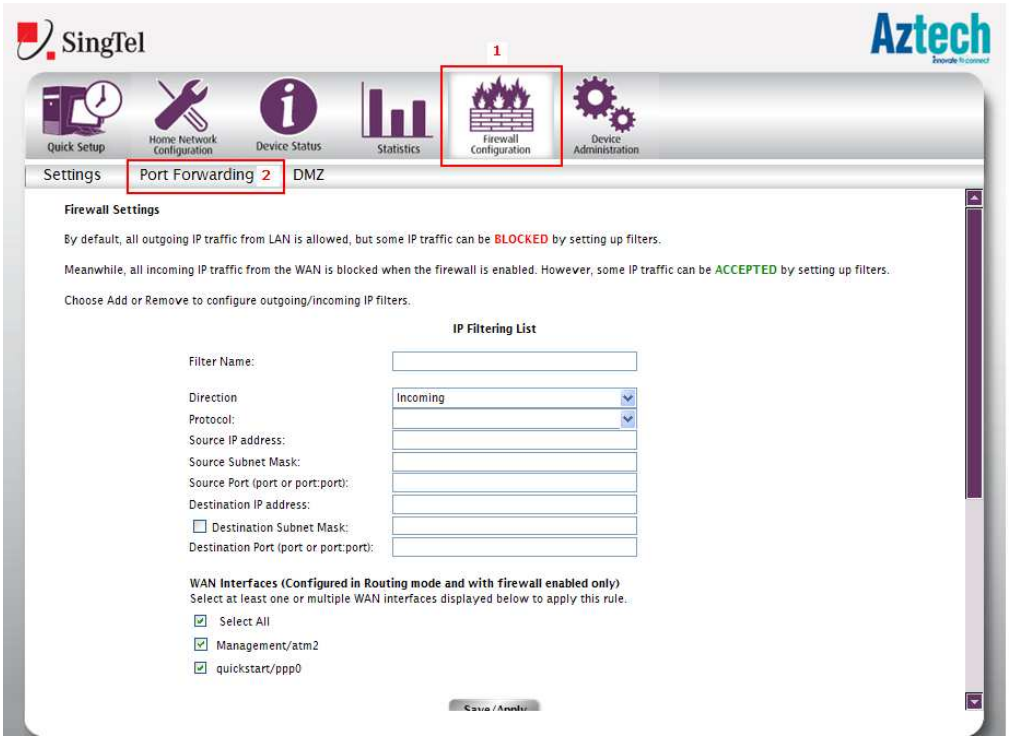
8. How I configure port Forwarding on my DSL1015EN(S)

1. Launch the Internet browser on your computer and input **192.168.1.254**. This will launch your Router's WEB User Interface.

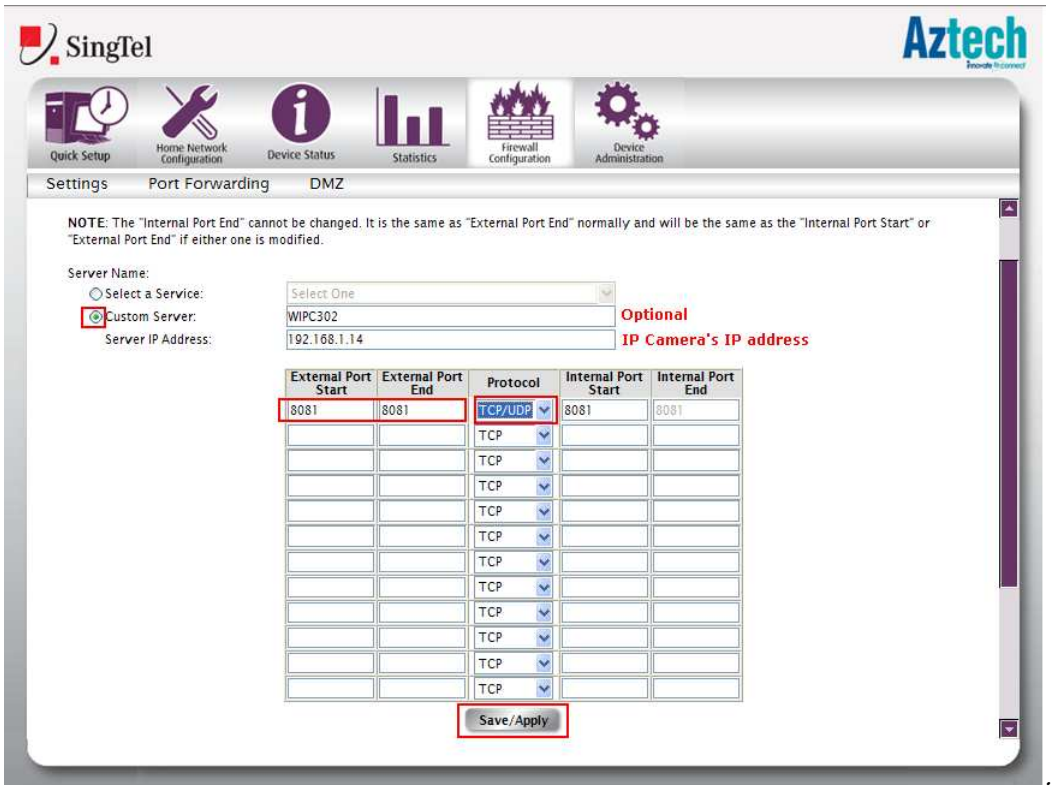


** Note that the login information is based on the default setting of the router.*

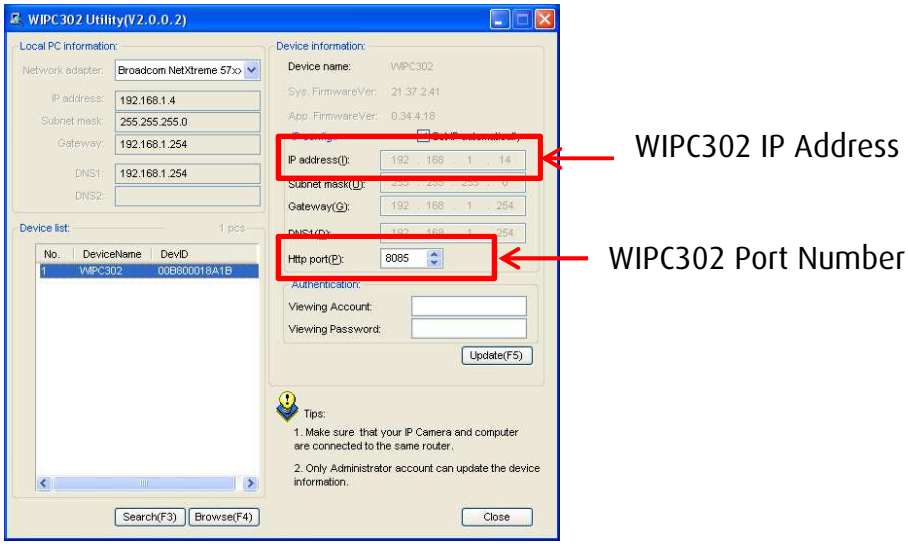
2. Click **Firewall Configuration** then click **Port Forwarding**.


SingTel
Aztech
1
Quick Setup
Home Network Configuration
Device Status
Statistics
Firewall Configuration
Device Administration
Settings
Port Forwarding 2
DMZ
Firewall Settings
By default, all outgoing IP traffic from LAN is allowed, but some IP traffic can be BLOCKED by setting up filters.
Meanwhile, all incoming IP traffic from the WAN is blocked when the firewall is enabled. However, some IP traffic can be ACCEPTED by setting up filters.
Choose Add or Remove to configure outgoing/incoming IP filters.
IP Filtering List
Filter Name:
Direction
Incoming
Protocol:
Source IP address:
Source Subnet Mask:
Source Port (port or port:port):
Destination IP address:
Destination Subnet Mask:
Destination Port (port or port:port):
WAN Interfaces (Configured in Routing mode and with firewall enabled only)
Select at least one or multiple WAN interfaces displayed below to apply this rule.
Select All
Management/atm2
quickstart/ppp0

3. Click **Customer Server** then input the **IP camera's name**. Under **Server IP address** Input the IP camera's IP address. Input the IP Camera's Port number under **External Port Start and End** then select the **TCP/UDP** under the **Protocol** drop down box.

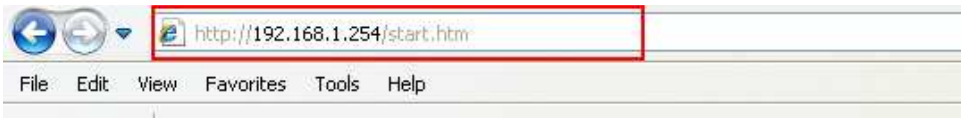


4. You may use the WIPC302 Utility to confirm the IP camera's IP address and Port number. Click **Save/Apply** on your DSL1015EW(S) for the settings to take effect.

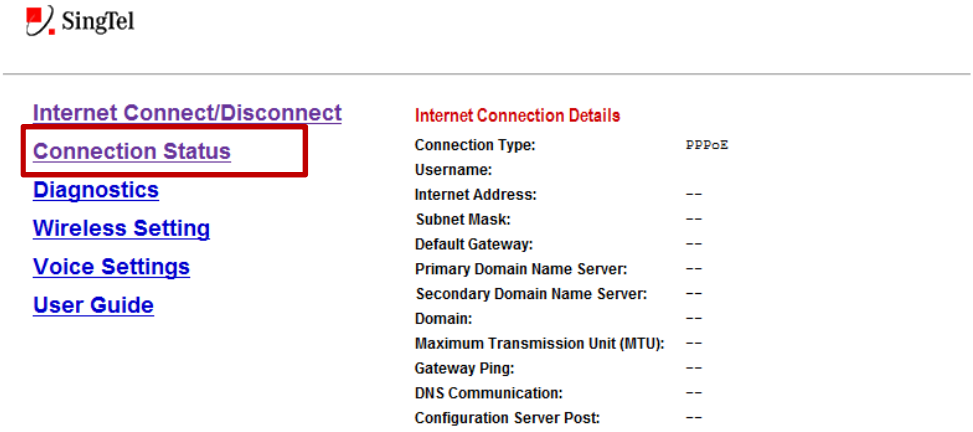


9. How I configure port Forwarding on my 2700HGV-2/2701HGV-E

1. Launch the Internet browser on your computer and input **192.168.1.254**. This will launch your Router's WEB User Interface.

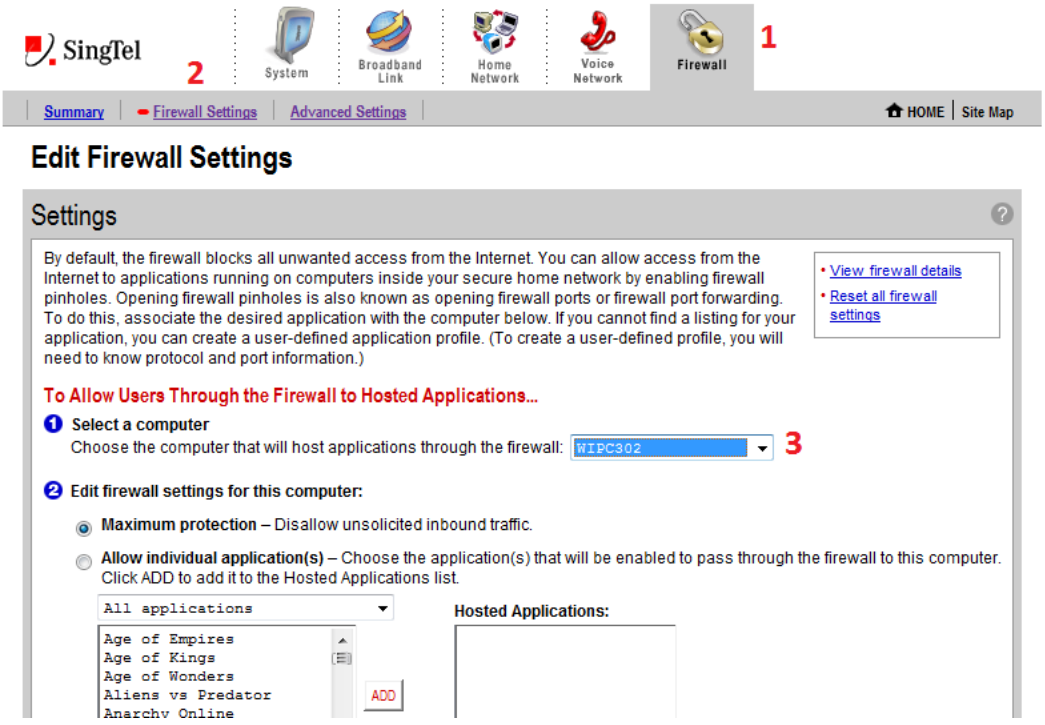


2. Click **Connection Status**, this will launch the configuration page.

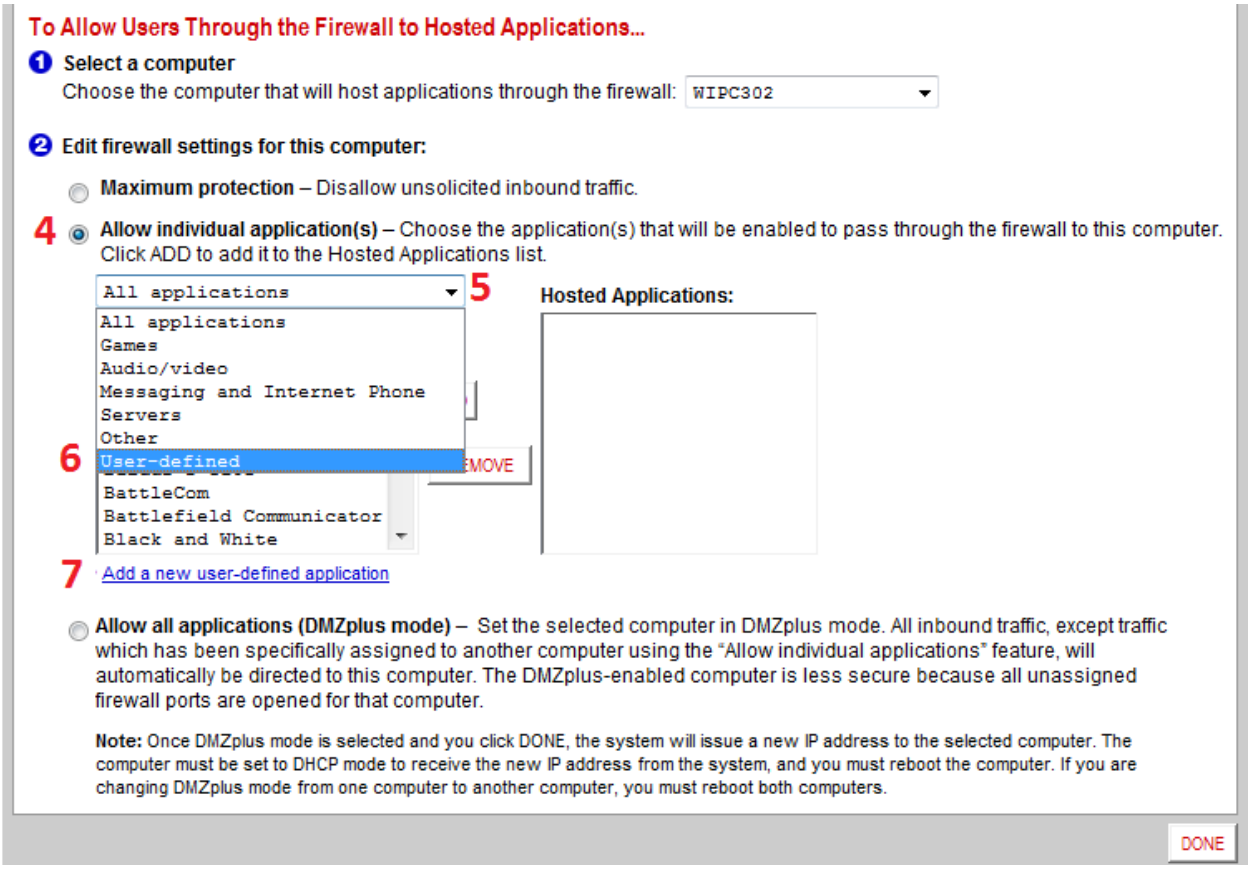


** Note that the login information is based on the default setting of the router.*

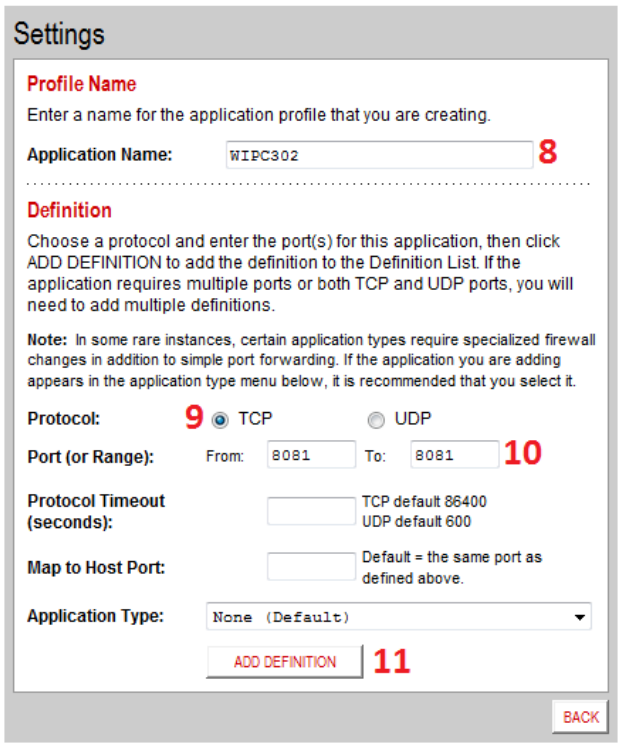
3. Select **Firewall** Tab and click **Firewall Settings** link then under **Select a computer** drop down link select WIPC302.


SingTel
2
System
Broadband Link
Home Network
Voice Network
Firewall
1
Summary
Firewall Settings
Advanced Settings
HOME
Site Map
Edit Firewall Settings
Settings
By default, the firewall blocks all unwanted access from the Internet. You can allow access from the Internet to applications running on computers inside your secure home network by enabling firewall pinholes. Opening firewall pinholes is also known as opening firewall ports or firewall port forwarding. To do this, associate the desired application with the computer below. If you cannot find a listing for your application, you can create a user-defined application profile. (To create a user-defined profile, you will need to know protocol and port information.)
View firewall details
Reset all firewall settings
To Allow Users Through the Firewall to Hosted Applications...
1 Select a computer
Choose the computer that will host applications through the firewall: WIPC302
3
2 Edit firewall settings for this computer:
Maximum protection – Disallow unsolicited inbound traffic.
Allow individual application(s) – Choose the application(s) that will be enabled to pass through the firewall to this computer. Click ADD to add it to the Hosted Applications list.
All applications
Age of Empires
Age of Kings
Age of Wonders
Aliens vs Predator
Anarchy Online
ADD
Hosted Applications:

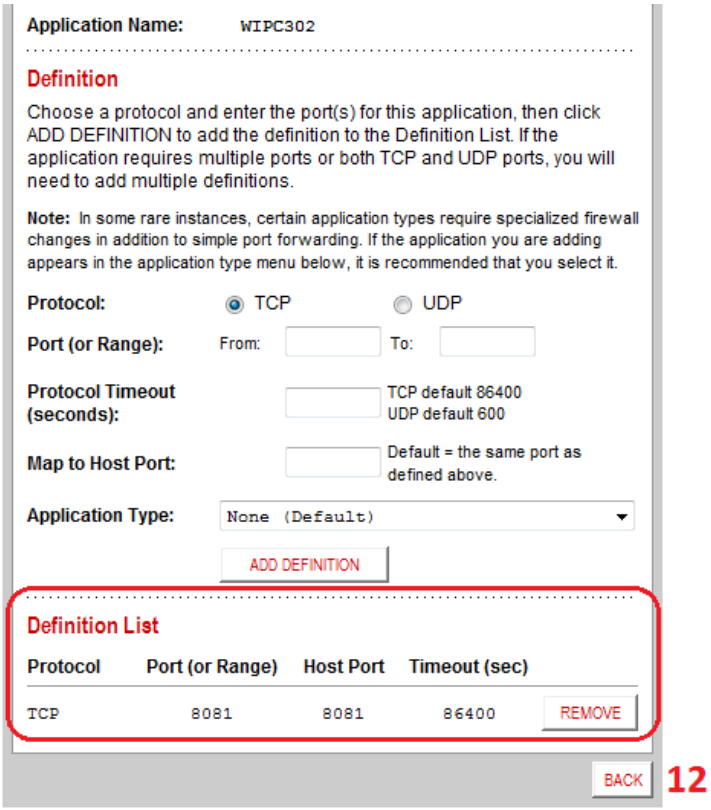
4. Click **Allow individual application(s)** and select **User-defined** from the drop down box then click **Add a new user-defined application**.


To Allow Users Through the Firewall to Hosted Applications...
1 Select a computer
Choose the computer that will host applications through the firewall: WIPC302
2 Edit firewall settings for this computer:
Maximum protection – Disallow unsolicited inbound traffic.
4
Allow individual application(s) – Choose the application(s) that will be enabled to pass through the firewall to this computer. Click ADD to add it to the Hosted Applications list.
All applications
5
Hosted Applications:
All applications
Games
Audio/video
Messaging and Internet Phone
Servers
Other
6
User-defined
BattleCom
Battlefield Communicator
Black and White
7
Add a new user-defined application
Allow all applications (DMZplus mode) – Set the selected computer in DMZplus mode. All inbound traffic, except traffic which has been specifically assigned to another computer using the "Allow individual applications" feature, will automatically be directed to this computer. The DMZplus-enabled computer is less secure because all unassigned firewall ports are opened for that computer.
Note: Once DMZplus mode is selected and you click DONE, the system will issue a new IP address to the selected computer. The computer must be set to DHCP mode to receive the new IP address from the system, and you must reboot the computer. If you are changing DMZplus mode from one computer to another computer, you must reboot both computers.
DONE

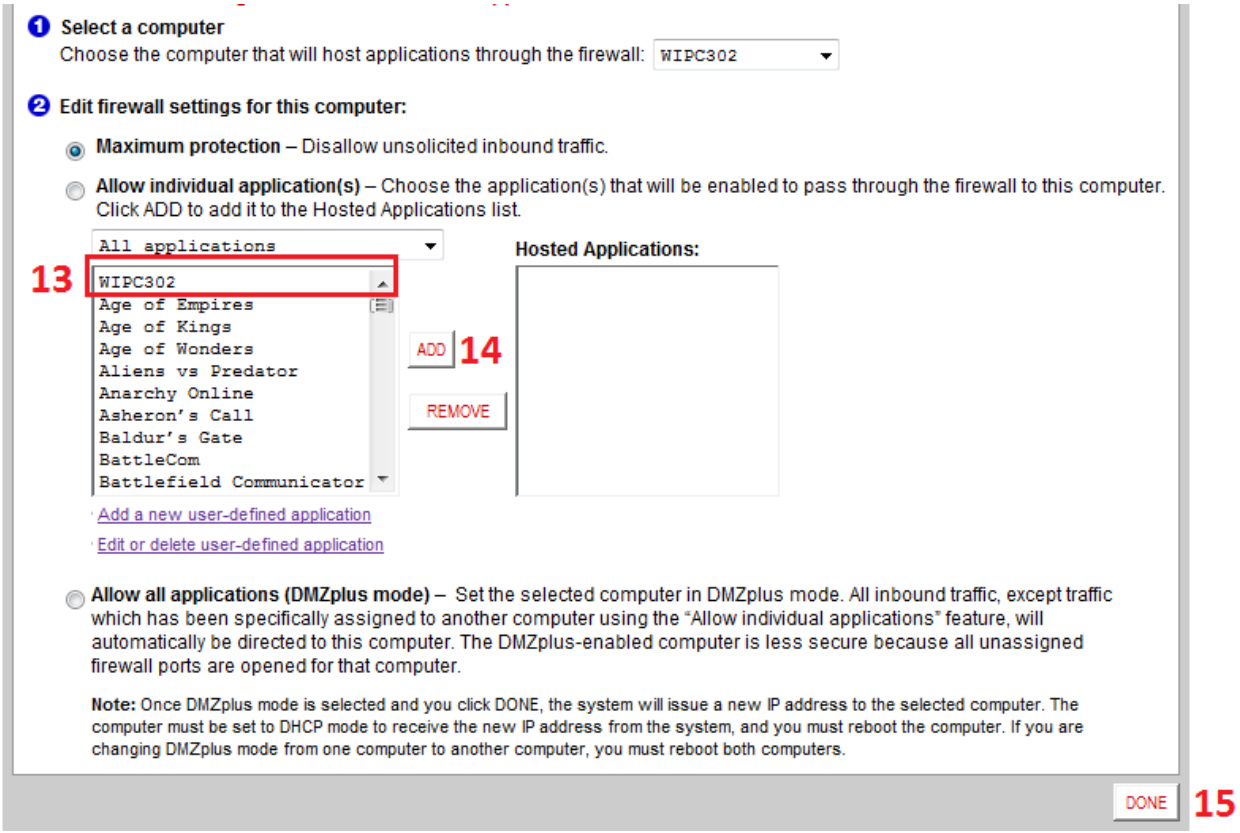
5. On the **Application Name** box input the IP camera's Name, select **TCP** on the **Protocol** option. Input **8081** on under **the Port (or Range)** field then click **ADD DEFINITION**.


Settings
Profile Name
Enter a name for the application profile that you are creating.
Application Name:
WIPC302
8
Definition
Choose a protocol and enter the port(s) for this application, then click ADD DEFINITION to add the definition to the Definition List. If the application requires multiple ports or both TCP and UDP ports, you will need to add multiple definitions.
Note: In some rare instances, certain application types require specialized firewall changes in addition to simple port forwarding. If the application you are adding appears in the application type menu below, it is recommended that you select it.
Protocol:
9
TCP
UDP
Port (or Range):
From:
8081
To:
8081
10
Protocol Timeout (seconds):
TCP default 86400
UDP default 600
Map to Host Port:
Default = the same port as defined above.
Application Type:
None (Default)
ADD DEFINITION
11
BACK

6. WIPC302 IP camera configuration will be added on the **Definition List** table. Click **Back** to return the Firmware Settings.


Application Name:
WIPC302
Definition
Choose a protocol and enter the port(s) for this application, then click ADD DEFINITION to add the definition to the Definition List. If the application requires multiple ports or both TCP and UDP ports, you will need to add multiple definitions.
Note: In some rare instances, certain application types require specialized firewall changes in addition to simple port forwarding. If the application you are adding appears in the application type menu below, it is recommended that you select it.
Protocol:
TCP
UDP
Port (or Range):
From:
To:
Protocol Timeout (seconds):
TCP default 86400
UDP default 600
Map to Host Port:
Default = the same port as defined above.
Application Type:
None (Default)
ADD DEFINITION
Definition List
Protocol
Port (or Range)
Host Port
Timeout (sec)
TCP
8081
8081
86400
REMOVE
BACK
12

7. Under the **All Application** box select the **WIPC302** then click **ADD** for the application to be added on the Hosted Application list. Click **DONE** for the settings to take effect.

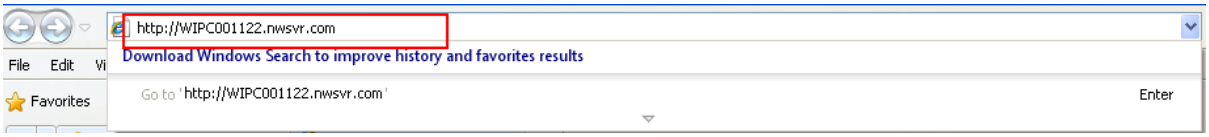

Select a computer
Choose the computer that will host applications through the firewall: WIPC302
Edit firewall settings for this computer:
Maximum protection – Disallow unsolicited inbound traffic.
Allow individual application(s) – Choose the application(s) that will be enabled to pass through the firewall to this computer. Click ADD to add it to the Hosted Applications list.
All applications
13
WIPC302
Age of Empires
Age of Kings
Age of Wonders
Aliens vs Predator
Anarchy Online
Asheron's Call
Baldur's Gate
BattleCom
Battlefield Communicator
ADD
14
REMOVE
Hosted Applications:
Add a new user-defined application
Edit or delete user-defined application
Allow all applications (DMZplus mode) – Set the selected computer in DMZplus mode. All inbound traffic, except traffic which has been specifically assigned to another computer using the "Allow individual applications" feature, will automatically be directed to this computer. The DMZplus-enabled computer is less secure because all unassigned firewall ports are opened for that computer.
Note: Once DMZplus mode is selected and you click DONE, the system will issue a new IP address to the selected computer. The computer must be set to DHCP mode to receive the new IP address from the system, and you must reboot the computer. If you are changing DMZplus mode from one computer to another computer, you must reboot both computers.
DONE
15

8. You may now access your IP camera via the internet using the Manufacturer's DDNS. Input http://WIPCxxxx.nwsvr.com (where xxxx is unique for every unit. Check the Manufacturer DDNS on the IP camera's WEB UI or on the label).

10. How do I access my IP camera on the laptop when I am not at home?

- You must have an Internet connection on your laptop when you are accessing the IP camera outside your house.
- Ensure that the DDNS information was set properly on the IP camera if you are using a Third Party DDNS else use the Manufacturer's DDNS.
- Port Forwarding must be configured on the router refer on your router's User Manual on how to set Port forwarding.

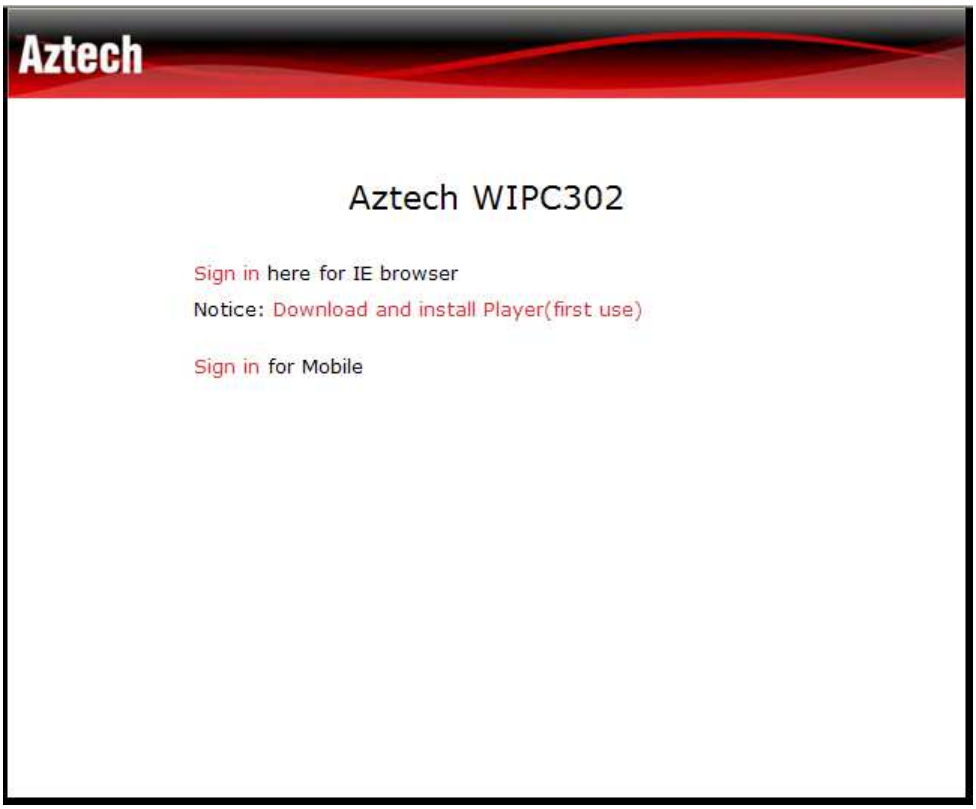
1. Launch the Internet browser on your notebook then input the IP camera's DDNS hostname



2. This will launch the authentication page, input the username and password that you set on the IP camera then click OK.

Connect to 192.168.3.3
The server 192.168.3.3 at ipcamera_00B800018A1B requires a username and password.
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).
User name:
admin
Password:
Remember my password
OK
Cancel

3. This will launch the IP camera's Home Page click Sign in to access the live video.


Aztech
Aztech WIPC302
Sign in here for IE browser
Notice: Download and install Player(first use)
Sign in for Mobile